Exhibit 1

FTI ™
CONSULTING

MAY 25, 2018

United States District Court
Southern District of Florida
Miami Division
CASE NO. 1:17-CV-60426-UU

ALEKSEJ GUBAREV, XBT HOLDING S.A., AND WEBZILLA, INC.,
PLAINTIFFS,
VS
BUZZFEED, INC. AND BEN SMITH,
DEFENDANTS

Expert report of
Anthony J. Ferrante
FTI Consulting, Inc.

Table of Contents

Qualifications

I am a Senior Managing Director and Global Head of Cybersecurity at FTI Consulting, Inc. ("FTI"). FTI is a global firm with over 3,600 professionals in 28 countries worldwide, specializing in forensic accounting, corporate restructuring, and litigation support services. The practice I lead at FTI provides expertise in cybersecurity resilience, prevention, response, remediation, and recovery services.

I have more than 15 years of top-level cybersecurity experience, providing incident response and preparedness planning to more than 1,000 private sector and government organizations, including over 175 Fortune 500 companies and 70 Fortune 100 companies.

I maintain operational knowledge of more than 60 criminal and national security cyber threat sets and have extensive practical expertise researching, designing, developing, and hacking complex technical applications and hardware systems.

Prior to joining FTI, I served as Director for Cyber Incident Response at the U.S. National Security Council at the White House where I coordinated U.S. response to unfolding domestic and international cybersecurity crises and issues. I led the development and implementation of Presidential Policy Directive 41 – United States Cyber Incident Coordination, the U.S. Government's national policy guiding cyber incident response efforts.

Before joining the National Security Council, I was Chief of Staff of the FBI's Cyber Division. I joined the FBI as a special agent in 2005 and was assigned to the FBI's New York Field Office. In 2006, I was selected as a member of the FBI's Cyber Action Team, a fly-team of experts who deploy globally to respond to the most critical cyber incidents on behalf of the U.S. Government.

I previously served as an Adjunct Professor of Computer Science at Fordham University's Graduate School of Arts and Sciences, where I served as the founder and co-director of the Master's of Science in Cybersecurity Program in the Graduate School of Arts and Sciences. During my time at Fordham University, I served as the co-director of the undergraduate and graduate cybersecurity research program.

My curriculum vitae is attached to this report as **Exhibit 1.**

Scope of Assignment

Davis Wright Tremaine LLP ("Counsel" or "DWT") retained FTI on August 16, 2017, in connection with Counsel's providing privileged and confidential legal advice to Counsel's clients, BuzzFeed, Inc. and Ben Smith, in the matter *Aleksej Gubarev, XBT Holding S.A. and Webzilla, Inc. v. BuzzFeed, Inc. and Ben Smith.*

I have prepared this expert report summarizing the investigation of statements in what is often referred to as the "Steele Dossier" ("Dossier") published by BuzzFeed in January 2017.

This report summarizes the key findings of the technical investigation into Aleksej Gubarev, XBT Holding S.A. ("XBT") and its subsidiaries, including the group of Gubarev web-hosting businesses that carry the name Webzilla.[1] FTI investigated the veracity of the Dossier's statements concerning the plaintiffs, as well as the same statements as applied to other subsidiaries of XBT. FTI also investigated information pertaining to the reputation, if any, of the plaintiffs, as well as other subsidiaries of XBT, for involvement in malicious cyber activity. Specific, high-priority objectives were to determine whether:

- Botnets and porn traffic hosted by XBT, Webzilla, and its affiliates facilitated theft of data from Democratic Party leadership;
- XBT, Webzilla, and their affiliates have a history of engaging in and/or hosting networks used by Russian state-sponsored malicious cyber activity; and
- XBT, Webzilla, and their affiliates have a history of, and reputation for, engaging in and/or hosting networks used for malicious cyber activity.

The investigation encompasses collection and analysis of information from an extensive range of open-source mediums. All sources relied upon in this investigation are cited in this report.

I may supplement and amend the opinions in this report in response to additional information received or to address issues raised by other witnesses.

---

1 XBT Holding, S.A. owns a series of companies that share the Webzilla name, both internationally and in the United States.

Glossary of Important Terms

Term[2]	Definition
Advanced Persistent Threat (APT)	A malicious attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.
Autonomous System (AS)	Collection of IP blocks under the control of one or more network operators, on behalf of a single administrative entity or domain.
Autonomous System Number (ASN)	A unique identifier assigned to each Autonomous System to differentiate between organizations and routing policies; analogous to a U.S. ZIP code.
Bot	A computer that has been compromised through a malware infection and can be controlled remotely by a cybercriminal.
Botnet	A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages.
Command-and-control server (C&C)	Centralized machines that are able to send commands and receive the output of machines that comprise a botnet.
COZY BEAR	A Russian hacker group believed to be associated with Russian intelligence. Classified as advanced persistent threat (APT) 29. Other monikers include Office Monkeys, CozyCar, The Dukes, and CozyDuke.
FANCY BEAR	A cyber espionage group. Classified as advanced persistent threat (APT) 28. Multiple security firms have assessed that it is associated with the Russian military intelligence agency GRU. Other monikers include Pawn Storm, Sofacy Group, Sednit and STRONTIUM.
Indicators of Compromise (IOCs)	Evidence of malicious activity on a system or network.
IP address	An identifier for a computer, server or other machine that is connected to the Internet, analogous to a postal address.

---

2 The glossary contains simplified definitions of technical terms for the benefit of readers unfamiliar with the subject matter.

Term[2]	Definition
IP block	An identifiable range of IP addresses. Also referred to as "netblock."
Ransomware	A type of malware that prevents or limits a user from accessing their server, network, computer or device either by locking the user's screen or by locking the user's files until a ransom is paid.
Root S.A.	XBT owned provider of Web Hosting, Dedicated Servers, Domain Names and many other Internet-related services.
Spambot	Program designed to collect email addresses from the Internet in order to send unsolicited email known as spam.
Secure Socket Layer (SSL)	A technology that establishes a secure session link between the visitor's web browser and the destination website so that all communications transmitted through this link are encrypted and are, therefore, secure.
Spear Phishing	The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.
Trojan	A type of malware that is often disguised as legitimate software designed to provide unauthorized, remote access to a user's server, network, computer or device.
Uniform Resource Locator (URL)	A protocol for specifying the address of a World Wide Web page.
URL Encoding	The practice of translating unprintable characters or characters with special meaning located within URLs to a format representation that is unambiguous and universally recognized by web browsers and servers.
Webazilla	The first iteration of a web-hosting brand which is now used by several subsidiaries of XBT.
Webzilla	The second iteration of the web-hosting brand which is now used by several subsidiaries of XBT, many of which are successor entities to Webazilla companies.
WHOIS	A standard protocol used to identify registered users of an

Term[2]	Definition
	Internet resource, such as a domain name, an IP address, or an autonomous system.
ZeuS Malware	Trojan malware package often used to steal banking information.

Executive Summary

This section summarizes the key findings of the investigation. Additional information for each finding, including citations and supporting exhibits, can be found in the Investigative Findings section of this report.[3]

- Technical evidence suggests that Russian cyber espionage groups used XBT infrastructure to support malicious spear phishing campaigns against the Democratic Party leadership which resulted in the theft of emails from a senior member of the Hillary Clinton presidential campaign.

- Technical evidence suggests that the Russian cyber espionage group that has been linked to the Democratic National Committee (DNC) hack has used an XBT-owned IP address in the past.

- Data published by U.S Government intelligence agencies suggests that XBT-owned infrastructure has been used for Russian military and intelligence intrusions of websites and computer systems for U.S. Government agencies, election commissions, think tanks, universities and/or corporations.

- Technical evidence suggests that XBT-owned infrastructure has been used to support malicious cyber campaigns tied to Russian cyber espionage and Advanced Persistent Threat (APT) actors.

- XBT-owned IP addresses have been used to support a number of high-profile malicious schemes and cyberattacks on critical infrastructure networks across the globe.

- A significant number of XBT-owned IP addresses were used to support the operation of a digital ad fraud scheme executed by Russian cybercriminals that was used to siphon millions of advertising dollars away from U.S. media companies.

- Depositions of key XBT executives and a review of communications produced show that XBT does not have an adequate enterprise infrastructure monitoring process in place or a formally defined procedure to investigate abuse notifications, which allows their infrastructure to be used without fear of repercussions.

- Public records research identified credible sources naming XBT affiliates as being involved in adverse, malicious or criminal cyber activity.


3 The phrases "announced IP address," "owned IP address," "originated IP address," and "leased IP address" can be used interchangeably. XBT personnel are responsible for originating the IP address for the purposes of connecting to the Internet.

Methodology

Technical Investigation

FTI's investigation into XBT infrastructure and cyber activity is based on a three-step approach:

1) Use third-party tools to identify all publicly available IP addresses and infrastructure that are hosted by XBT subsidiaries;

2) Compare the infrastructure hosted by XBT to government and private security firm threat intelligence repositories of IP addresses, domains, and malware samples known to propagate malicious cyber activity; and[4]

3) Review and investigate all matches to determine the type and nature of malicious activity or ties to the hack of Democratic Party leadership and other interference in the 2016 U.S. election.

Identify XBT affiliated IPs and Infrastructure → Compare to Threat intelligence Repository → Analyze Matches
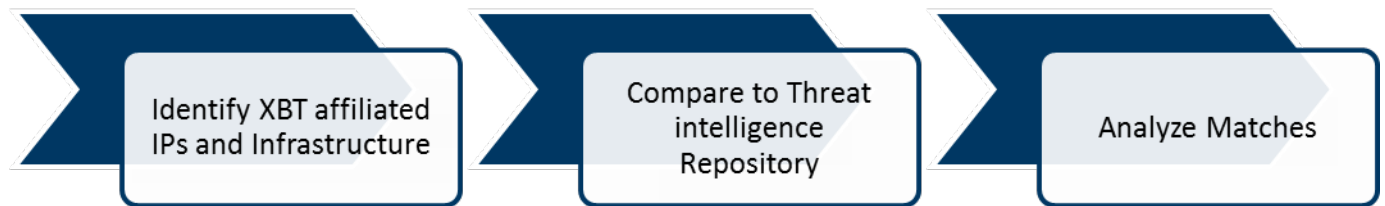
FTI's methodology is further detailed throughout this report.

---

[4] Threat intelligence data used in our report comes from the various private security firms and government agencies referenced throughout the report. All firms are reputable within the security industry.

Investigative Findings

Background and Approach

XBT's primary business is providing web-hosting and network solutions for its customers. XBT subsidiaries lease data centers and infrastructure in various geographic locations, including the U.S., Europe, and Asia.

For important context on the investigation of malicious cyber activity, FTI highlights the following three key technical concepts for Hosting ISPs:

- **Internet Protocol Addresses ("IP")**

- **Autonomous Systems ("AS")**

- **Autonomous System Numbers ("ASN")**

In understanding these concepts, it can be useful to think of the Internet in terms of old-fashioned mail delivery. IP addresses are unique numbers assigned to all individual parts of the Internet – the lines of communication over which online information flows. IP addresses, then, represent a kind of physical mailing address that identifies the location of specific websites, computers, or other machines attached to the Internet. Autonomous Systems are the backbone of the Internet because they contain collections of IP addresses under the control of an entity that presents clearly defined gateways to the Internet. Autonomous System Numbers are unique identifiers for each Autonomous System and, in turn, are analogous to a ZIP code that helps Autonomous Systems route information to the proper IP addresses across the Internet.

Understanding this Internet routing system allows investigators to map data flow on the Internet – from specific IP addresses, associated with an Autonomous System Number, and originating from an identifiable Autonomous System. XBT subsidiary entities are assigned a unique and officially registered Autonomous System Number – their own, specific ZIP code. These ASNs are important from an investigative standpoint because they allow investigators to identify the exact originating networks for IP addresses. Hence, when malicious Internet activity is identified, investigators can link that activity and its IP address, to an ASN, and through that number to the assigned Autonomous System of the offending IP address.[5]

---

[5] Threat intelligence reports and repositories are created by various private security firms and government agencies to track sources, metadata and organizations behind malicious cyber campaigns. These reports and repositories contain listings of Indicators of Compromise ("IOCs") associated with malicious cyber activity. IOCs can include the domain, underlying IP address, malware sample hash or other identifying technical component. Cybersecurity experts, including myself, regularly rely on this information in our work.
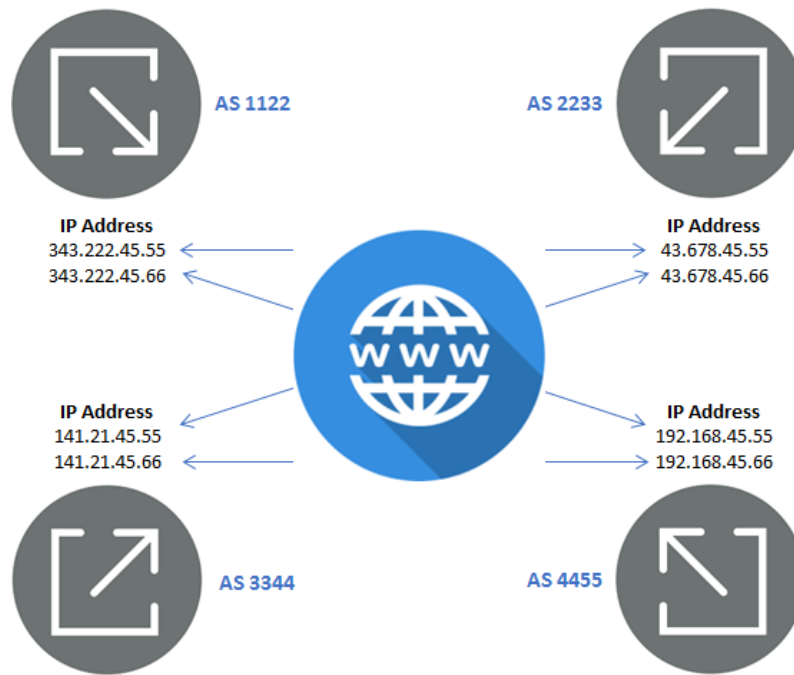
The image above illustrates how Autonomous Systems support the Internet.

Overview of ASN Infrastructure

FTI uses third-party solutions Shodan and RipeStat to identify the ASNs and IP addresses owned by a given entity, based on the registered domain.[6] [7] FTI's analysis indicates that XBT infrastructure hosts 782 distinct IP prefixes and up to 1,418,783 IP addresses.[8] [9] These IP addresses are linked to 12 Autonomous Server Numbers owned by XBT and its subsidiary entities:[10] [11]

ASN ID	XBT - Owned Companies	# of Distinct IP Prefixes	# of Distinct IP Addresses
7979	Servers.com, Inc.	134	724,992
40824	WZ Communications, Inc.	231	362,496
5577	Root S.A.	82	156,416
35415	Webzilla B.V.	216	132,102
45470	8-to-infinity Pte Ltd (Webzilla Singapore)	28	8,960
48792	Webazilla B.V.	1	8,192
39134	Edinaya Set	37	6,937

6 Shodan "crawls" the Internet for publicly accessible devices, including Web servers. From a technical perspective, the tool scans the Internet for all publicly available servers and probes each port on that server to see what, if any, service is running.
7 The RIPE NCC collects and stores Internet routing data from locations around the globe, using the Routing Information Service established in 2001. RIS data can be accessed via stat.ripe.net, a repository on current and historical Internet number resources.
8 The number of active IP addresses as of January 10, 2018. The metrics include active and historical IP information.
9 All prefixes that were ever announced on an XBT affiliated ASN were captured in the review.
10 Refer to Exhibit 2.
11 All XBT-owned companies are listed on the XBT Holding SA-2016 Consolidated.pdf, page 11 (P-G000390).

ASN ID	XBT - Owned Companies	# of Distinct IP Prefixes	# of Distinct IP Addresses
46786	IP Transit Inc.	21	6,656
40431	Travail Systems	19	6,400
58909	IBEE Software Solutions Ltd	3	3,072
7177	DFW Internet Services, Inc.	9	2,304
61107	Universal CDN	1	256

The number of active IP addresses available within an individual ASN can change frequently. Administrators from web-hosting companies can originate (i.e. "announce") or withdraw IPs within a given ASN – effectively turning the IP addresses on or off – by altering the configurations on what are called gateway routers. Throughout this investigation, FTI leveraged Shodan and RipeStat to update the listing of all IP addresses affiliated with Autonomous System Numbers owned by XBT and to review relevant historical information. These IP addresses are the base dataset tested against threat intelligence sources to identify malicious activity tied to XBT. FTI further investigated matches by using WHOIS to determine the entity or individual that registered the IP address.[12] For historical analysis, RipeStat was used to validate the ASN where an IP was announced at a specific point in time.

The Democratic Party Hacks

FTI investigated whether it could find any technical connections between XBT and the allegations made in the Dossier about XBT and its affiliates, including Webzilla, by analyzing technical data published by government agencies, third party security firms or produced in response to a subpoena request. The Dossier states:

"a company called XBT/Webzilla and its affiliates had been using botnets and porn traffic to transmit viruses, plant bugs, steal data and conduct "'altering operations'" against the Democratic Party leadership. Entities linked to one Aleksej GUBAROV were involved and he and another hacking expert, both recruited under duress by the FSB, Seva KAPSUGOVICH, were significant players in this operation." [13]

The private security firm CrowdStrike was contracted by the DNC to investigate the hack on its infrastructure.[14] In June 2016, CrowdStrike published an analysis, "Bears in the Midst: Intrusion into the Democratic National Committee," that included indicators of compromise (IOCs) and technical information on how Russian cyber espionage groups COZY BEAR (also known as APT29) and FANCY BEAR (also known as APT28) infiltrated the DNC network. According to the CrowdStrike report, both of these actors engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's intelligence services. The report also

---

12 WHOIS is a query and response protocol that is widely used for querying public databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. FTI uses https://centralops.net/co/domaindossier.aspx to review IP registration data.

13 https://www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html

14 CrowdStrike, Inc. is an American cybersecurity technology and threat intelligence company based in Sunnyvale, California.

states that FANCY BEAR frequently registers domains that closely resemble legitimate companies and then establishes fake websites on these domains that spoof the look and feel of the victim's email in order to steal their credentials. [15]

Another component of the Democratic Party hack was a malicious spear phishing attack launched against the Hillary Clinton presidential campaign and Democratic Party leadership. The attack was launched by FANCY BEAR starting in March 2016 and continued through at least April 2016. Emails designed to look like they came from Google, the company that provided the Clinton campaign's email infrastructure, were sent to campaign staff with '@hillaryclinton.com' email addresses. The email messages requested users to enhance their security or change their passwords by clicking on a URL embedded in the phishing email. When users clicked on the embedded URL it launched a fake website designed to collect their email username and password (i.e., user credentials). The spear phishing attack used a service called Bitly to shorten the length of and thereby disguise malicious URLs embedded in phishing emails. [16] [17]

The Bitly Link

Technical evidence suggests that FANCY BEAR used XBT infrastructure to support malicious spear phishing campaigns against the Democratic Party leadership. Based on documents published by WikiLeaks, on March 19, 2016 an email was sent to Clinton campaign manager John Podesta, requesting that he change his email password by clicking on an embedded icon that read, "Change Password." The icon was actually a bitlink (https://bit[.]ly/1PibSU0) which, when clicked, launched a fake website apparently designed to look like a Google security page requesting the user enter their user credentials.[18] The WikiLeaks posting stated that Podesta clicked on the bitlink and entered his user credentials. At that point, FANCY BEAR had access to Podesta's emails.[19] [20]

Documents produced by Bitly in response to a subpoena show that the company conducted an internal investigation of how Bitly was used in the spear phishing attack of the DNC and Democratic Party leadership.[21] Bitly's investigation found that the account 'john356gh' was used to create the bitlink embedded in the phishing email sent to John Podesta. Further review showed that the account created 11,139 bitlinks from 10/20/2015 through 6/30/2016 using 41 distinct IP addresses. Bitly's analysis of the underlying URLs disguised by the shortened bitlinks showed that six URLs contained "dnc.org" and 95 contained "hillaryclinton.com," which indicates the spear phishing was targeting individuals across the Democratic Party. [22]

---

15 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (Exhibit 3)
16 https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a
17 Bitly is a tool that allows users to shorten website addresses (URLs) and is primarily used for social media and marketing campaigns. It has been used by cybercriminals to disguise malicious URLs.
18 Links created by Bitly are referred to as "bitlinks."
19 https://wikileaks.org/podesta-emails/emailid/34899
20 A spear phishing attack is an email scam targeted towards an individual, organization or business in an attempt to steal information or install malware. Email messages are disguised to look like they were sent by a trustworthy entity and entice recipients to click on a website link or provide sensitive personal information.
21 Refer to Exhibit 4.
22 ibid

The URL underlying the bitlink sent to John Podesta's email contained encoding that, when translated, included "John," "John Podesta," "John.Podesta@gmail.com," and a link to a professional photo of John Podesta. This link is no longer active and cannot be found in Internet archives, but this encoding provides strong technical evidence that it was a phishing (i.e., fake) website apparently designed to look like a real Google security page and customized to deceive John Podesta into providing his email credentials.[23]

Bitly produced a system audit log of the 11,139 bitlinks created by john356gh which included the bitlink, date created, underlying URL (i.e., website) and the IP address used to create the bitlink.[24] FTI could not establish a technical connection between the IP address used to create https://bit[.]ly/1PibSU that John Podesta clicked on and XBT. However, using the signatures and data contained in the bitlink that John Podesta clicked on, FTI identified three additional phishing websites in the john356gh account audit log data designed to look like custom Google security pages for John Podesta. **One of those bitlinks was created by an IP address owned by Root S.A., 94.242.205[.]147.**[25] The table below compares the bitlink that was sent in a phishing email and used to steal John Podesta emails (Column A) to a bitlink created by a Root S.A. IP address (Column B):[26]

Data Element	Column A	Column B
Bitlink	https://bit[.]ly/1PibSU0	http://bit[.]ly/22KAIn8
Underlying URL	http://**myaccount.google.com**/ecuritysettingpage[.]tk/**security/signinoptions**/password?e=**am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D**&fn=**Sm9obiBQb2Rlc3Rh**&n=**Sm9obg%3D%3D**&img=**Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFFCTS9CQldVOVV0bUZUWQUWS9waG90by5qcGc%3D**&id=1sutlodlwe	http://**myaccount.google.com**-0b31hojr8d20uc3rhcnrlcl9mawxl0b31hojr8d20uc3rhcnrlcl9mawxl[.]tk/**security/signinoptions**/password?e=**am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D**&fn=**Sm9obiBQb2Rlc3Rh**&n=**Sm9obg%3D%3D**&img=**Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFFCTS9CQldVOVV0bUZUWQUWS9waG90by5qcGc%3D**&id=3le696uvbt&continue=https://myaccount.google.com
URL Encoding	- base64.b64decode(params['n'][0]) = 'John' - base64.b64decode(params['fn'][0]) = 'John Podesta' - base64.b64decode(params['e'][0]) = 'john.podesta@gmail.com' - base64.b64decode(params['img'][0]) = '//lh4.googleusercontent.com/-QeYOlrdTjvY/AAAAAAAAAAI/AAAAAAA	- base64.b64decode(params['n'][0]) = 'John' - base64.b64decode(params['fn'][0]) = 'John Podesta' - base64.b64decode(params['e'][0]) = 'john.podesta@gmail.com' - base64.b64decode(params['img'][0]) = '//lh4.googleusercontent.com/-QeYOlrdTjvY/AAAAAAAAAAI/AAAAAAA

---

23 ibid
24 Refer to Exhibit 5.
25 https://stat.ripe.net/widget/routing-history#w.resource=94.242.205.147
26 CONFIDENTIAL-BITLY_00032_john356gh_audit_bitlink_history_alternate.csv, row 7246

Data Element	Column A	Column B
	AABM/BBWU9T4mFTY/photo.jpg'	AABM/BBWU9T4mFTY/photo.jpg'
IP Address	85.17.82[.]165 (Leaseweb)	94.242.205[.]147 (Root S.A.)
Date Created	2016-03-19	2016-04-19

The underlying URLs share the same phishing signatures, both appear to be fake google websites that abuse Open Authentication (OAuth).[27] These are phishing signatures are attributed to Fancy Bear based on an April 2017 report published by security firm Trend Micro.[28] [29] [30] Additionally, the URL encoded values in the table above suggest that the fake website was designed specifically for John Podesta in order to steal information from him. Based on information currently available, FTI cannot definitively state that the bitlink created using the Root S.A. IP address was ever sent to or received by John Podesta. However, these technical indicators show that the phishing URL underlying the abovementioned bitlink was created with the intent to steal John Podesta's email credentials as part of the cyber operations launched against the DNC and Democratic Party leadership.

Additional Technical Connections

Technical evidence suggests that FANCY BEAR may have used an IP address owned by XBT subsidiary, Root S.A., in the past. The CrowdStrike report included seven command-and-control (C&C) IP addresses and five malware hashes (i.e., malicious software programs) as the IOCs in the DNC hack. FTI reviewed the IP registration information for the seven C&C IP addresses but none were affiliated with XBT. Similarly, FTI was not able to identify a direct technical connection to XBT infrastructure based on an analysis of the five malware samples. However, **FTI found an indirect link between FANCY BEAR and XBT infrastructure through a Secure Socket Layer (SSL) certificate used by two of the C&C IPs listed in the CrowdStrike IOCs.**[31]

SSL certificates are used for authentication and data encryption. Administrators for web servers will create SSL certificates and distribute those certificates to other servers or Internet devices that they trust to communicate with it. Two IP addresses listed in the CrowdStrike IOCs use the same SSL certificate which

---

27 OAuth (Open Authorization) is an open standard for token-based authentication and authorization on the Internet.
28 Refer to Exhibit 28.
29 Trend Micro Inc. is a Japanese multinational cyber security & defense company founded in Los Angeles, California.
30 Phishing Signatures are common data points or methods that enable investigators to determine if phishing emails are tied to the same attack.
31 SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

suggests that the certificate is controlled by FANCY BEAR. Ownership of SSL certificates cannot be transferred; indicating that the SSL certificate used to control the IPs listed in the Crowdstrike report has always been controlled by FANCY BEAR. Further review found that the SSL certificate has been distributed to 40 other IP addresses and that one of those is owned by Root S.A (**94.242.224[.]172**).[32] Please refer to the image below for additional technical information.
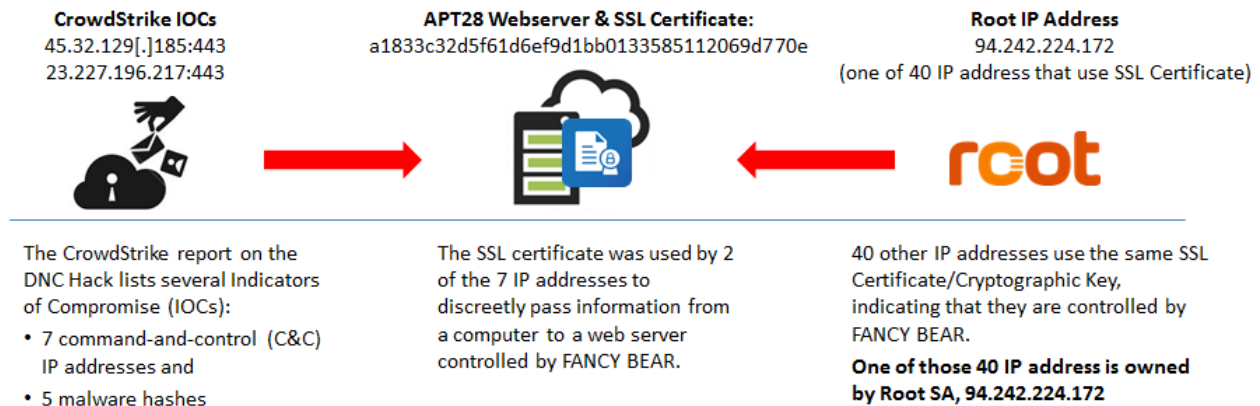
FTI notes that because this is an indirect link, more data from CrowdStrike and/or the DNC is required to determine if XBT infrastructure supported the DNC Hack.[33]

Other U.S. Election Meddling

Technical evidence suggests that IP addresses owned by Root S.A. were included in the tools and infrastructure used by Russian intelligence to interfere in the 2016 U.S. Election. The Department of Homeland Security ("DHS") and Federal Bureau of Investigation ("FBI") released Joint Analysis Report JAR-16-20296A, codenamed "Grizzly Steppe," in response to Russian interference in the 2016 election. The report "provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services ("RIS") to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities."[34] The Grizzly Steppe report includes IOCs associated with RIS cyber actors.[35]

The findings of the report indicate that two RIS actors participated in the Democratic Party hack. The first actor group, COZY BEAR, entered into the party's systems in the summer of 2015, while the second, FANCY BEAR, entered during the spring of 2016. In the past, both groups have targeted government organizations, universities, and private corporations around the world.

FTI identified 13 IP addresses listed in the Grizzly Steppe report that are owned by XBT subsidiary Root S.A.

---

32 https://stat.ripe.net/widget/routing-history#w.resource=94.242.224.172
33 Refer to Exhibit 6.
34 https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (Exhibit 7).
35 https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity (Exhibit 7).

IP	CIDR	ASN	NETNAME	COUNTRY
212.117.180[.]130	212.117.160.0/19	5577	ROOT, LU	LU
212.117.180[.]21	212.117.160.0/19	5577	ROOT, LU	LU
94.242.195[.]186	94.242.192.0/18	5577	ROOT, LU	LU
94.242.206[.]196	94.242.192.0/18	5577	ROOT, LU	LU
94.242.222[.]23	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]162	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]163	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]165	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]177	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]181	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]183	94.242.192.0/18	5577	ROOT, LU	LU
94.242.239[.]189	94.242.192.0/18	5577	ROOT, LU	LU
94.242.251[.]32	94.242.192.0/18	5577	ROOT, LU	LU

These findings indicate RIS actors have utilized XBT-owned infrastructure.[36]

Documents produced by the plaintiff illustrate that minimal, if any, internal investigation was performed by the company into the IP addresses noted on the Grizzly Steppe Report on a timely basis. In an email chain produced during discovery, Konstantin Bezruchenko, CTO of XBT, sent an email to Marc Goederich, Managing Director of Root S.A., asking about abuse notifications or requests Root S.A. received from "local police or other EU/U.S. law enforcement agencies" for the IP addresses noted in government reports. The email from Bezruchenko was dated September 6, 2017, nine months after the Grizzly Steppe report was released. Goederich forwarded an email he received from the Luxembourgish authorities on December 30, 2016 seeking information on what data they maintained for IP address **212.117.180[.]21**. Goederich responded that the IP is a "tor exit node" and "doesn't get us very far."[37] [38] Additionally, a Cybersecurity Specialist for the Luxembourgish government contacted Goederich on January 3, 2017 asking "could you check on what these 3 IPs are? They have come up in the report from the DHS regarding the Russian attacks." Goederich responded that "most have been clients for quite a long time and have more than one server, so really something more like resellers."[39] Based on our experience, this is not an adequate response to a government inquiry. Goederich provided additional information on each IP address to Bezruchenko and Gubarev, such as those that were TOR Exit nodes, and stats on the abuse notifications for the IP addresses noted in the table above.[40] It does not appear that Goederich took any other steps to investigate the IP addresses noted in the report. However, FTI was able to identify the following

---

36 Refer to Exhibit 8.
37 P-T000012 through P-T000015.
38 Tor is software and a network for enabling anonymous communication, directing Internet traffic through a worldwide, volunteer network. Refer to Statements from Deposition Testimony for more information.
39 P-T000020
40 P-T001712.

information from the abuse notifications produced by XBT and to which Goederich would have had easy access:

- On May 16, 2014 the Threat and Vulnerability Management Team at Betfair submitted an abuse request for **94.242.239[.]163** noting that it was habitually scanning their network. The abuse notification was captured in Root S.A ticking work flow and sent to the end customer. A response was provided by king.servers1@gmailcom stating that the IP address was a Virtual Private Network (VPN) service and that it was closed.[41] [42]

- On June 6, 2014 an abuse notification was submitted for **94.242.239[.]181** at Leadads.com stating that the IP was trying to hack their tracking system. The abuse notification was captured in Root S.A ticking work flow and sent to the end customer.   A response was provided by king.servers1@gmailcom stating that the IP address was a VPN service and that it was closed.[43]

Vladimir Fomenko is the owner of King Servers, a Russia-based web-hosting company. ThreatConnect identified six domains owned by King Servers that had been used to infiltrate the Arizona and Illinois State Boards of Elections.[44] In December 2016, Russian authorities arrested two senior FSB officers and an executive at Kaspersky Labs and charged them with treason. The independent Russian newspaper Novaya Gazeta reported that the accused men provided U.S officials with information about Fomenko. FTI was not able to link King Server infrastructure to XBT, but these abuse notifications suggest that King Servers was a customer of Root S.A.[45] The ThreatConnect report was published in September 2016, a few months before the December 2016 publication of the Grizzly Steppe report and the 13 Root S.A. IP addresses. In our experience it's highly unusual that the connection would not have been made between the ThreatConnect report and the Root S.A. IP addresses apparently used by King Servers.

Neither of the IP addresses noted above was identified by Goederich as TOR exit nodes. **Based on this evidence, it does not appear that an internal investigation was performed by XBT in the weeks after the publication of the Grizzly Steppe report. Based on industry experience, it would be highly unusual not to conduct an investigation into infrastructure components noted in government reports as propagating malicious activity, if the operators were concerned about running a lawful, legitimate service.**

The Methbot Operation

The Russian Methbot Advertising Fraud Operation ("Methbot") was run from mid-2015 through December 2016 by Russian cybercriminals and involved siphoning millions of advertising dollars away from U.S. media companies. White Ops, a cybersecurity company that protects digital advertisers from ad fraud and other automated threats, published a white paper on December 20, 2016 on Methbot. The white paper provides technical information on the advanced botnet operation, its estimated financial impact and related IOCs. The white paper stated that "Methbot was the largest and most profitable advertising fraud operation to

---

41 P-T001704 through P-T001706.

42 A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

43 P-T001714 through P-T001717.

44 https://threatconnect.com/blog/state-board-election-rabbit-hole/

45 https://www.cyberscoop.com/russia-fsb-arrests-king-servers-threatconnect/

strike digital advertising to date."[46]   The operation produced massive volumes of fraudulent video advertising impressions by commandeering Internet infrastructure and targeting video advertising. A so-called army of web browsers spoofed advertisers into believing their ads were being viewed millions of times per day on fake sites controlled by online fraudsters. Those fake views attracted real advertising dollars – reportedly as much as $5 million per day – that were then funneled to the criminals.[47]

The infrastructure behind the Methbot operation included more than 850,000 IP addresses supported by an estimated 800 to 1,200 dedicated servers located in the U.S. and the Netherlands.[48] The advanced techniques included faked clicks, mouse movements, and social network login data to masquerade as engaged human consumers. The Methbot fraud also included sophisticated manipulation of IP geolocation information.[49]

Traditional bots use existing IP addresses by compromising individual computers. However, that structure limits the amount of "clicks" or "views" that can be performed. The Methbot operation was executed across a distributed network based on a custom browser engine running out of a data center using IP addresses with forged registration data. The Methbot operation was first detected in September 2016 and expanded aggressively in October 2016, according to White Ops.

FTI obtained and reviewed historical data associated with XBT-owned ASNs and IP blocks – in layman's terms, these are ranges of IP addresses.[50] The XBT-owned IP prefixes were compared against the IOCs published by White Ops in order to determine whether XBT infrastructure could be linked to the Methbot operation. FTI found evidence to support that 24% of the IP prefixes and up to 78% of IP addresses associated with the Servers.com ASN AS7979 were included in the Methbot IOCs. Additionally, evidence supports that 69% of the IP prefixes and up to 74% of IPs affiliated with the WZ Communications ASN AS40824 were included in the Methbot IOCs.[51]

Below is a breakdown by XBT entity.

XBT Entity	IP Prefixes			IP Addresses		
	Total #	Methbot Linked	% of Total	Max Total #	Methbot Linked	% of Max Total
WZ Com Inc. (AS40824)	207	142	68.5	357,120	264,192	74
Servers.com (AS7979)	66	16	24.2	379,136	296,960	78.3
Total	**273**	**158**	**57.8**	**736,256**	**561,152**	**76.2**

An analysis of historical data using RipeStat shows that Methbot IP addresses originated and began scaling up on Servers.com ASNs in late September and October 2016. Methbot IP addresses began originating on

---

46 https://www.whiteops.com/methbot (Exhibit 9).
47 ibid
48 A dedicated server is a single computer in a network reserved for serving the needs of the network.
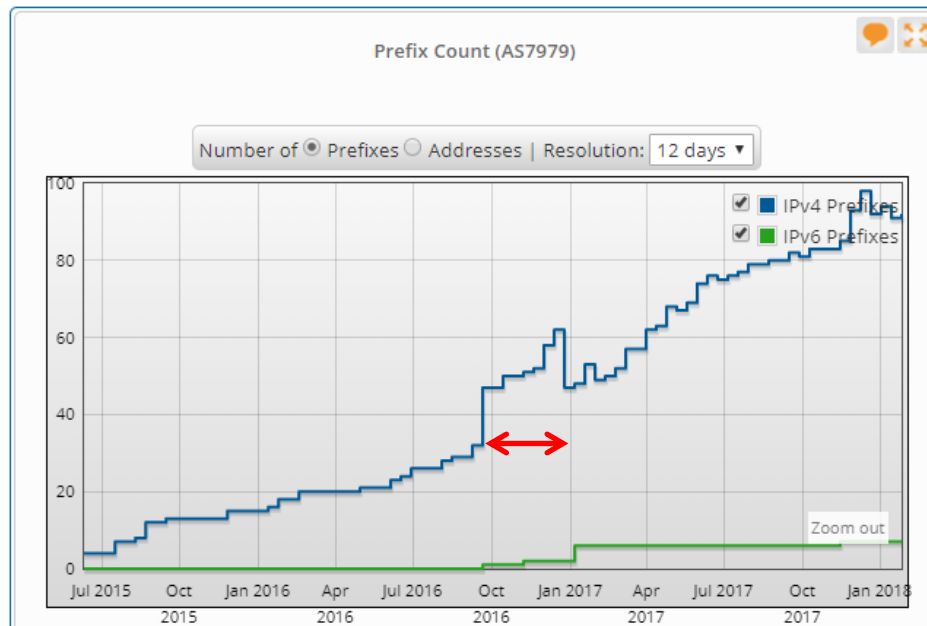49 ibid
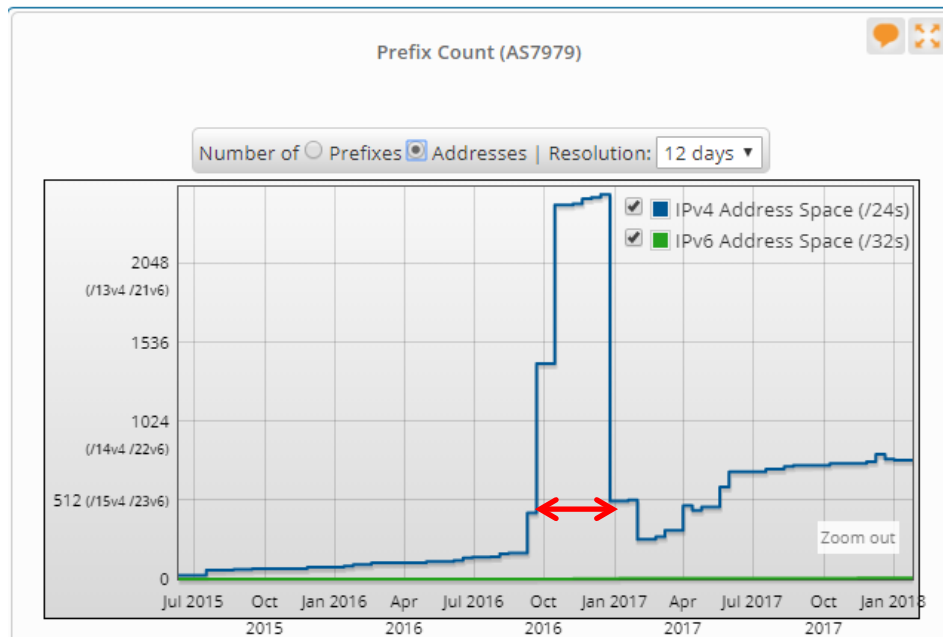50 Methbot historical data and other technical information can be found in Exhibit 10.
51 FTI notes that not all Methbot IP addresses within a given IP prefix were assigned to an XBT entity during the Methbot Operation.

WZ Communications in October 2015, although they did not experience the same scale of IP origination (i.e., growth).
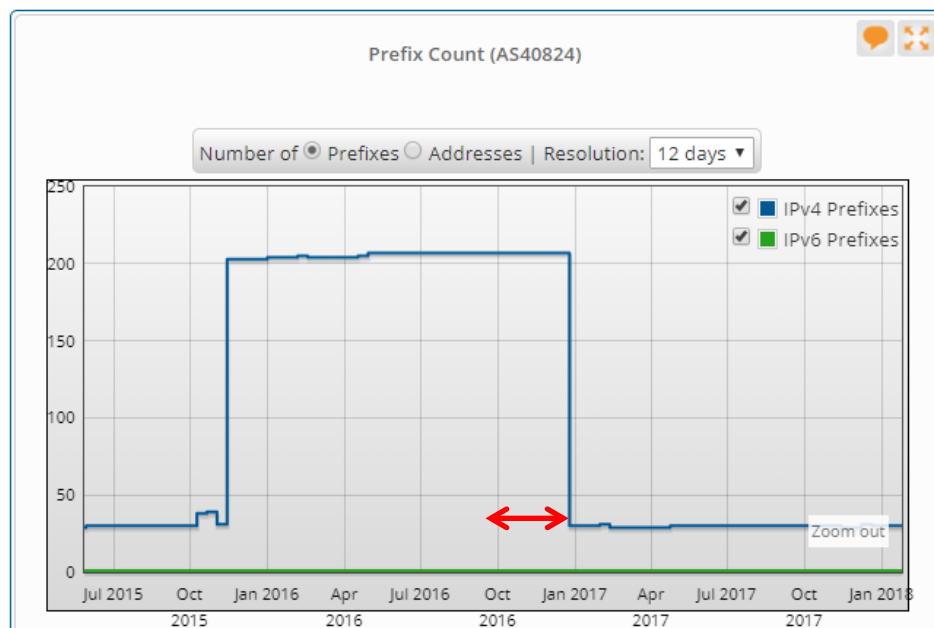
The timeframe for the large increase in IP addresses for Servers.com is significant because it is consistent with the timeframe when the Methbot operation began to "scale aggressively," according to the White Ops paper. FTI notes that both Servers.com and WZ Communications abruptly withdrew Methbot IP addresses on December 25, 2016, five days after White Ops released their report on the Methbot operation. According to RipeStat, on December 25, 2016, the number of announced IP prefixes on the Servers.com ASN went from 61 to 47, and the number of announced IP prefixes on the WZ communications ASN went from 200 to 30.

The graph from https://stat.ripe.net/ illustrates the significant increase of **IP prefixes** originating on the Servers.com ASN starting in late September and October 2016 and the corresponding withdrawal of **IP prefixes** in late December 2016, days after the White Ops report was released. The red line represents the period when the operation "scaled aggressively."
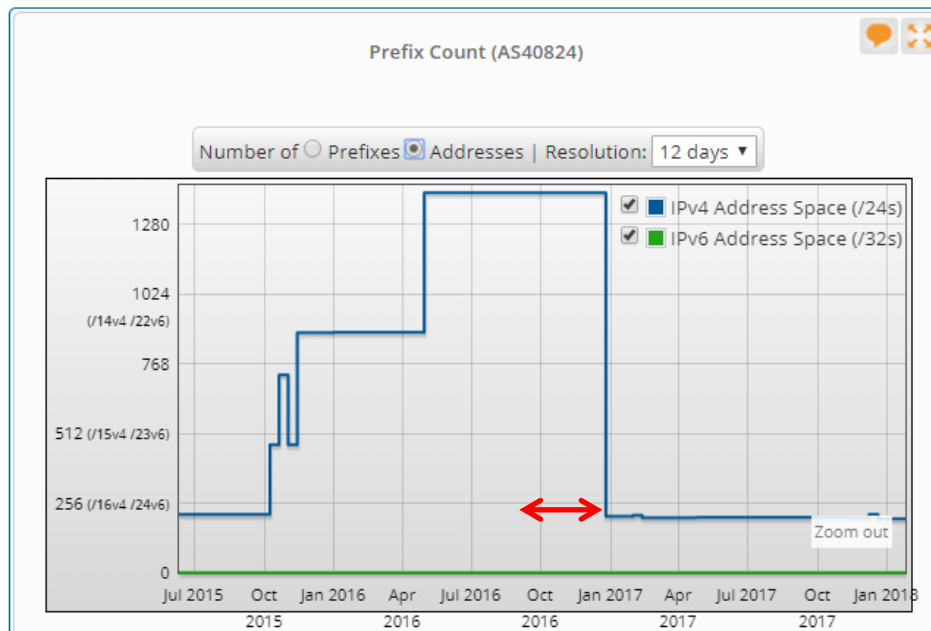
The graph from https://stat.ripe.net/ illustrates the significant increase of **IP addresses** originating on the Servers.com ASN starting in late September and October 2016 and the corresponding withdrawal of **IP addresses** in late December 2016, days after the White Ops report was released. The red line represents the period when the operation "scaled aggressively."

The graph from https://stat.ripe.net/ illustrates the significant increase of **IP prefixes** originating on the WZ Communications ASN starting in October 2015 and the corresponding withdrawal of **IP prefixes** in late December 2016, days after the White Ops report was released. The red line represents the period when the operation "scaled aggressively."

The graph from https://stat.ripe.net/ illustrates the significant increase of **IP addresses** originating on the WZ Communications ASN starting in October 2015 and the corresponding withdrawal of **IP addresses** in late December 2016, days after the White Ops report was released. The red line represents the period when the operation "scaled aggressively."

The dramatic origination and subsequent withdrawal of IP addresses can only be performed manually, by configuring the Border Gateway Protocol ("BGP") settings on the physical routers. A network administrator or someone with knowledge of the infrastructure at both Servers.com and WZ Communications would have had to manually change the BGP configurations on December 25, 2016 to withdraw these IP addresses.

The high number of technical connections to the Methbot Operation IOCs and the dramatic fluctuations in Methbot-linked IP addresses indicates that individuals affiliated with Servers.com and WZ Communications may have been aware XBT-related infrastructure was used for an illegal operation. Additionally, the operation was a large scale "botnet", which is consistent with statements made in the Dossier.

Documentation produced by the plaintiffs provides evidence that XBT became aware of the Methbot Operation after the White Ops report was released and took action to terminate the responsible customer. This is likely the reason why FTI observed the withdrawal of IP addresses noted above in late December 2016. Gubarev said in emails that he and other employees knew the customer "personally" for "many years," and that the customer has been to Cyprus several times. He was using "over 1000 servers," "everybody" at the company interacted with him because he was a "big client," and Gubarev spoke with him personally. The client had represented that he was a "big data analytics system" for video ads.[52] However, when asked to provide a copy of the contract with the customer in question Gubarev responded "due to fact we know this customer we do not ask him to sign contract by mistake as a result we can't claim damages." Gubarev also estimated that the company will lose between "2-2.5M$" if they could not resell the servers.[53] That represents between 4% and 5% of the 2016 XBT revenue according to the XBT 2016

---

[52] P-P001536.
[53] KGlobal 001041.

Consolidated Financial Statement.[54] **It is a highly unusual and risky business practice for hosting companies to provide services without signed contracts, especially instances when the customer is requesting a large number of servers and the company is at risk of losing a large amount of revenue.**

Malicious Cyber Activity

XBT-owned infrastructure has been used to support malicious cyber campaigns tied to Russian state actors, high-profile malicious schemes and cyber attacks on critical infrastructure networks across the globe. This section details the key findings FTI identified based on an extensive review of government and private security firm reports.[55]

Technical Connections to Russian State Actors

CRASHOVERRIDE & Ukraine Power Grid Attack

The Ukrainian power grid was the victim of a cyber-attack in December 2015. Hackers were able to compromise the information systems of three energy distribution companies and disrupt the electricity supply from these entities for approximately one hour. After another attack in 2016, the United States Department of Homeland Security, National Cybersecurity and Communications Integration Center ("NCCIC") issued Alert TA17-163A (referencing the "CRASHOVERRIDE" malware) about the power-grid attacks.[56] Private security firms ESET and Dragos, Inc. subsequently published a collaborative report with more information on the CRASHOVERRIDE malware used to take control of Ukrainian industrial information systems. This new type of attack campaign was dubbed "CRASHOVERRIDE" malware because of its ability to disrupt key infrastructure. According to the ESET and Dragos report, the cyber-attack on Ukraine "marked a revolutionary event for electric grid operators. It was the first known instance where a cyber-attack had disrupted electric grid operations."[57] [58] [59]

Based on the report issued by Dragos and ESET, the adversary group behind CRASHOVERRIDE was identified as ELECTRUM. The private security firms also assessed with high confidence that ELECTRUM has direct ties to the Sandworm team, a cyber espionage group with ties to Russia.[60] [61]

FTI reviewed the IOCs issued in NCCIC Alert TA17-163A and identified a total of five IP addresses used to support the attack. **One of those five IP addresses was owned by an XBT subsidiary business entity, 8-to-**

---

54 XBT Holding SA- 2016 Consolidated.pdf, page 11 (P-G000365 - P-G000405).

55 Unless otherwise noted, government and private security firm reports did not specifically reference XBT entities. FTI established the connections to XBT-owned IP addresses using WHOIS and RipeStat.

56 https://www.us-cert.gov/ncas/alerts/TA17-163A (Exhibit 11).

57 https://dragos.com/blog/CRASHOVERRIDE/CRASHOVERRIDE-01.pdf (Exhibit 27)

58 Dragos, Inc. is an industrial cybersecurity company based out of Hanover, Maryland, which is focused on industrial environments such as those found in industrial control system (ICS), Supervisory Control and Data Acquisition (SCADA), and Distributed Control System (DCS) environments.

59 ESET is an IT security company that offers anti-virus, and firewall hardware products, as well as Managed Service solutions. The company is headquartered in Bratislava, Slovakia.

60 https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National-Security/Graphics/briefing2.pdf

61 https://dragos.com/blog/crashoverride/

Infinity Pte, Ltd. XBT acquired 8-to-Infinity Pte, Ltd. in 2012, reportedly to expand its holdings and operations in Asia.[62] The company in October 2013 changed its name to Webzilla Singapore PTE Ltd. IP address 188.42.253[.]43 is still registered to 8-to-Infinity but now belongs to an IP block associated with XBT subsidiary Root S.A. per public IP registration data.[63]

The table below illustrates the ASN and IP addresses used to support the 2015 Ukraine attack. The 8-to-Infinity/Root S.A. IP address is highlighted in red.

AS	IP	BGP Prefix	AS Name
59939	195.16.88[.]6	195.16.88.0/22	WIBO-AS, LT
197988	46.28.200[.]132	46.28.200.0/21	SOLARCOM, CH
45470	188.42.253[.]43	188.42.252.0/22	SG-8-TO-SG 8-to-Infinity Pte Ltd, SG
57043	5.39.218[.]152	5.39.218.0/24	HOSTKEY-AS, NL
16125	93.115.27[.]57	93.115.24.0/21	CHERRYSERVERS1-AS, LT

Win32/Industoyer Malware

An ESET white paper published in June 2017 identified that same Root S.A. owned IP address cited in the CRASHOVERRIDE report had been used as a command-and-control server for the "Win32/Industroyer" malware software. Win32/Industroyer is a sophisticated piece of malware designed to disrupt industrial control systems, specifically those used in electrical substations.[64] Once an industrial control system is infected by the malware, the attackers can remotely control systems such as switches and circuit breakers from command-and-control servers. ESET states that Win32/Industroyer may have been the tool that attackers used to cause a power outage in the Ukraine in December 2016.[65] [66] ESET did not attribute the use of Win32/Industroyer to any specific threat groups. However, the malware does share signatures with the Black Energy Trojan malware which has been attributed to Sandworm, a Russian cyber espionage group.[67]

CosmicDuke Malware

In a September 2014 white paper about COZY BEAR, cybersecurity firm F-Secure identified that Root S.A. owned IP address **94.242.199[.]88** was used as a command-and-control server for the COZY BEAR-designed "CosmicDuke" malware.[68] [69] [70] When active, the CosmicDuke malware will search for and harvest login credentials from a variety of programs, collect information from those programs and forward that data to

---

62 http://www.thewhir.com/web-hosting-news/xbt-holding-expands-with-acquisition-of-singapore-web-host-8-to-infinity
63 https://stat.ripe.net/widget/routing-history#w.resource=188.42.253.43
64 https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf (Exhibit 12).
65 ibid
66 https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA
67 BlackEnergy is a Trojan malware designed to launch distributed denial-of-service (DDoS) attacks, download custom spam, and banking information-stealer plugins. BlackEnergy malware was known to have been used to deliver KillDisk, a feature that could render systems unusable. It is reported to have possessed remarkable functions that could place Industrial Control Systems (ICS) at risk. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-BlackEnergy
68 F-Secure Corporation is a Finnish cyber security and privacy company based in Helsinki, Finland.
69 https://www.f-secure.com/documents/996508/1030745/cosmicduke_whitepaper.pdf (Exhibit 13).
70 https://stat.ripe.net/widget/routing-history#w.resource=94.242.199.88

its own servers.[71]   As noted in previous sections of this report, COZY BEAR is a Russian hacker group believed to be associated with Russian intelligence.

Technical Connections to APT Careto

In 2014, Kaspersky Lab listed Webzilla Singapore owned IP address **223.25.232[.]161** a server used by Careto, an APT actor that has been operating since at least 2007.[72] [73]   According to Kaspersky's *Unveiling "Careto" – The Masked APT*, Careto may be a nation-state sponsored campaign due to its sophisticated techniques.   However, intelligence and security firms have not stated what country they are affiliated with. When active in a system, Careto's malware can intercept network traffic, keystrokes, Skype conversations, PGP keys, analyze Wi-Fi traffic, fetch all information from Nokia devices, screen captures and monitor all file operations.   The Kaspersky white paper indicates that the identified IP address is a command-and-control "exploit staging server IP," indicating it was a key part of the attack.[74]

Operation Potao Express

A July 2015 white paper titled "Operation Potao Express" published by cybersecurity firm ESET listed Root S.A. owned IP address **94.242.199[.]78** as a command-and-control server for the malware known as "win32/Potao"(part of the "Potao" malware family).[75] [76]   The Potao malware family shares many characteristics with the BlackEnergy Trojan, which has been used by the Sandworm team, a cyber espionage group with ties to Russia.[77]   Both Potao and BlackEnergy malware have been used in attacks against Ukrainian government and military institutions.   The Potao malware family was active as early as August 2011, when it was used in a "mass spreading" campaign infecting targets in several countries.   ESET stated that the Potao malware family was still very active at the time the white paper was published.[78]

Sedreco

An October 2016 report titled "En Route with Sednit" published by ESET listed URL **updatesystems[.]net** as a command-and-control domain for a backdoor malware identified as "Sedreco."   The URL resolves to the 8-to-Infinity owned IP address **188.42.254[.]26**.[79] [80]   The malware is believed to be created by FANCY BEAR (i.e., Sednit) and allows for persistent access to a victim's network for the attacker.[81]

---

71 https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf
72 Kaspersky Lab is a multinational cybersecurity and anti-virus provider headquartered in Moscow, Russia and operated by a holding company in the United Kingdom. Kaspersky Lab develops and sells antivirus, internet security, password management, endpoint security, and other cybersecurity products and services.
73 https://stat.ripe.net/widget/routing-history#w.resource=223.25.232.161
74 https://app.box.com/s/aepgdq5vc2dxd2m9t0ab2v28rtwbhjua (Exhibit 14).
75 https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf (Exhibit 15).
76 https://stat.ripe.net/widget/routing-history#w.resource=94.242.199.78
77 https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/14/National Security/Graphics/briefing2.pdf
78 https://www.welivesecurity.com/wp-content/uploads/2015/07/Operation-Potao-Express_final_v2.pdf
79 https://stat.ripe.net/widget/routing-history#w.resource=188.42.254.26
80 Refer to Exhibit 16.
81 https://app.box.com/s/lmaensc7vzdugsy1nsh4bwligl07q53b (Exhibit 17).

Other Malicious Cyber Activity

The Gozi Malware (ISFP)

The Gozi malware is a computer virus that infected more than one million computers worldwide, enabling hackers to access personal bank information and to steal tens of millions of dollars from 2007 to 2011.[82] In 2012 the U.S. Attorney's Office for the Southern District of New York dubbed Gozi "one of the most financially destructive computer viruses in history."[83] Variants of the Gozi malware have continued to be used for subsequent malware campaigns. In September 2015, the Swiss government issued a CERT report on a "malvertising" campaign that compromised a popular advertising network in Switzerland and involved hundreds of thousands of possible victims from France and Germany. The malware was installed on end-user machines by exploiting vulnerabilities in Internet Explorer, Java and Adobe Flash. The malware behind the Swiss campaign was GOZI ISFP.[84] **FTI notes that a Root S.A. IP address, 94.242.254[.]208, supported the GOZI IFSP malware campaign and was identified as the possible command-and-control server for the attack**.[85] [86] [87]

FTI notes that documents produced by plaintiffs indicate that Gubarev, Constantin Luchian, and XBT subsidiaries have a business relationship with a Nikita Kuzmin, including purchasing assets from a company Kuzmin operated as recently as 2017. Kuzmin was president of ServerClub, Inc. which was registered in 2011 by Luchian and his company Incorporate Now. An individual with the same name is a convicted cybercriminal responsible for authoring the Gozi virus in 2007. Kostyantyn Bezruchenko confirmed in his deposition that he knew Kuzmin personally and that Kuzmin was in prison for illegal internet activities.[88]

RIG Exploit Kit (RIG)

The cyber threat-intelligence firm, Talos, monitors large malware campaigns and issues analysis and reports on those campaigns on a periodic basis.[89] In January 2016, Talos issued an analysis on the RIG Exploit Kit ("RIG"), a variation of a malicious tool commonly used to deliver banking Trojans or ransomware.[90] Talos' analysis of data obtained from September 1, 2015 through October 30, 2015, showed RIG was affecting

---

82 https://www.justice.gov/usao-sdny/pr/three-alleged-international-cyber-criminals-responsible-creating-and-distributing-virus
83 Ibid
84 GOZI IFSB is a variant of the original Gozi malware, which U.S. criminal courts determined was developed by Russian cybercriminal Nikita Kuzmin and his partners in 2006. Kuzmin in 2016 pleaded guilty to U.S. criminal charges related to his role in the Gozi campaign.
85 https://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan. (Exhibit 18). Please note that FTI is not able to confirm that Kuzmin or his known associates developed the Gozi ISFP variant that was referenced in the Swiss Cert Report.
86 A command-and-control server is a centralized machine used to issue commands to infected computers and gather misappropriated information from those computers (e.g. stolen credit card numbers).
87 https://stat.ripe.net/widget/routing-history#w.resource=94.242.254.208
88 Bezruchenko Dep. 305:3 – 315:8.
89 The Talos Intelligence Group researches and publishes reports regarding known and emerging threats, new vulnerabilities in common software, and other threats.
90 An exploit kit is software designed to run on web servers with the purpose of identifying software vulnerabilities (i.e. in Windows, Adobe, Java, etc.), uploading and executing malicious code to users (i.e. delivering "payloads"). Exploit kits are commonly used to deliver banking Trojans and/or ransomware.

hundreds of users per day, compared to thousands per day like other exploit kits. RIG was also delivering spambot malware, while other exploit kits were typically delivering Trojans or ransomware.[91] [92]

When Talos investigated the infrastructure supporting the RIG Exploit, the firm "observed 44 unique IP addresses delivering some form of RIG. On most days, there were only one or two IPs actively hosting RIG. When we resolved the IPs associated ASN, we found something surprising. With the exception of a single IP address, all IPs belonged to the same ASN (35415)." **The report noted that the ASN is owned by Webzilla, and by extension the IP addresses. The IP addresses associated with the Webzilla ASN in question were leased to a client business entity, Eurobyte, LLC.**[93] [94]

Talos reportedly contacted both Eurobyte and Webzilla in late 2015 and provided both companies with information about the hosts. According to Talos, Webzilla responded and blocked the customers that were generating the events. Despite multiple emails to communicate with Eurobyte, Talos reported RIG activity continued as new IP addresses were brought online. It is not clear, based on the Talos report or FTI's independent analysis, whether the servers that continued to host RIG were owned by XBT.

PonyUp Scheme

Pony is a form of malware, often delivered through phishing, that dates to at least 2013 and that has included multiple variations over time. Computer security firm Damballa issued a Threat Report in late 2015 titled *"PonyUp: Tracing Pony's Threat Cycle and Multi-Stage Infection Chain."*[95] The malicious spear phishing campaign detailed in the report enticed users into clicking on links and images in spam emails by impersonating well-known companies, using their logos and known subject lines to deceive the user. When a user clicked on an email, a malicious program was downloaded that allowed the hacker to steal data on the infected machine. **There were 20 IP addresses noted in the report that are believed to be used for command-and-control purposes. Seven of those 20 IP addresses are affiliated with Webzilla ASN 35415.**[96] [97]

AS	IP	BGP Prefix	AS Name
35415	109.234.34[.]57	109.234.34.0/24	WEBZILLA B.V.
35415	109.234.37[.]184	109.234.37.0/24	WEBZILLA B.V.
35415	178.208.78[.]76	178.208.78.0/24	WEBZILLA B.V.
35415	178.208.91[.]229	178.208.91.0/24	WEBZILLA B.V.
35415	206.54.183[.]106	206.54.183.0/24	WEBZILLA B.V.

---

91 A spambot is a malicious program designed to collect email addresses from the internet to build mailing lists.

92 A Trojan is any malicious program which misleads users from its true intent. Ransomware is a malicious program that encrypts data on the infected machine until a ransom is paid.

93 http://blog.talosintelligence.com/2016/01/rigging-compromise.html (Exhibit 19).

94 Webzilla is specifically listed in the report.

95 Damballa is a cyber security company, based out of Atlanta, GA, specializing in network monitoring for advanced threats. Damballa was acquired by Roswell Based Cybersecurity Organization Core Security in July 2016.

96 https://stat.ripe.net/widget/routing-history#w.resource=109.234.34.57; https://stat.ripe.net/widget/routing-history#w.resource=109.234.37.184; https://stat.ripe.net/widget/routing-history#w.resource=178.208.78.76; https://stat.ripe.net/widget/routing-history#w.resource=178.208.91.229; https://stat.ripe.net/widget/routing-history#w.resource=206.54.183.106; https://stat.ripe.net/widget/routing-history#w.resource=46.30.42.177; https://stat.ripe.net/widget/routing-history#w.resource=46.30.42.234

97 Webzilla B.V. was specifically referenced in the Damballa Report as the ASN associated to those seven IP addresses.

AS	IP	BGP Prefix	AS Name
35415	46.30.42[.]177	46.30.42.0/24	WEBZILLA B.V.
35415	46.30.42[.]234	46.30.42.0/24	WEBZILLA B.V.
43449	91.194.254[.]224	91.194.254.0/23	DIMLINE-AS Dimline Ltd.
43449	91.194.254[.]236	91.194.254.0/23	DIMLINE-AS Dimline Ltd.
43449	91.194.254[.]82	91.194.254.0/23	DIMLINE-AS Dimline Ltd.
44050	31.184.192[.]214	31.184.192.0/19	PIN-AS Petersburg Internet Network LLC
44050	91.220.131[.]109	91.220.131.0/24	PIN-AS Petersburg Internet Network LLC
44050	91.220.131[.]16	91.220.131.0/24	PIN-AS Petersburg Internet Network LLC
44050	91.220.131[.]241	91.220.131.0/24	PIN-AS Petersburg Internet Network LLC
48031	46.161.40[.]108	46.161.40.0/24	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich
48031	91.217.90[.]137	91.217.90.0/23	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich
48031	91.226.212[.]142	91.226.212.0/23	XSERVER-IP-NETWORK-AS PE Ivanov Vitaliy Sergeevich
197695	151.248.113[.]8	151.248.113.0/24	AS-REGRU _Domain names registrar REG[.]ru_
197695	5.63.154[.]158	5.63.154.0/24	AS-REGRU _Domain names registrar REG[.]ru_
201094	185.86.76[.]168	185.86.76.0/22	GMHOST Alexander Mulgin Serginovic

The report concluded that the PonyUp scheme was orchestrated by well-organized criminals. The criminals behind the campaign relied on a network of so-called "bulletproof hosts" to create botnets quickly and effectively. Bulletproof hosting is a service provided by domain-hosting or web-hosting firms that allows their customer considerable leniency in the kinds of material they may upload and distributed. This leniency has been taken advantage of by spammers and by illicit online gambling and illegal pornography sites.[98]

Darkhotel

A November 2014 report titled "Darkhotel Indicators of Compromise" published by Kaspersky listed URL **autosail[.]ns01[.]biz** as a command-and-control server for the malicious campaign referred to as "Darkhotel."[99] This URL resolves to Root S.A. owned IP address **94.242.199[.]172**.[100] [101] Darkhotel is a targeted spear phishing, spyware and malware-spreading campaign that selectively attacks business hotel visitors through the hotel's in-house Wi-Fi network in an attempt to steal sensitive information. The Kaspersky report states that the IP address was hosting the malicious URL as part of this group's efforts to target guests of hotels in Asia.[102]

---

98 Refer to Exhibit 20.
99 https://app.box.com/s/r97cjt70ywsd7pnrstr7buqzxn5svfw1 (Exhibit 21)
100 https://stat.ripe.net/widget/routing-history#w.resource=94.242.199.172
101 Refer to Exhibit 22.
102 ibid

Technical Links to APT Nitro

A 2014 Palo Alto Networks report about the group known as "Nitro" listed URL **good[.]myftp[.]org** as a command-and-control URL used by the threat actor group to support malicious attacks.[103]   The URL resolves to the 8-to-Infinity owned IP address **223.25.233[.]248**.[104] [105]   This group is known for spear phishing attacks but has recently used compromised legitimate websites to gain access and steal information from victims.   The report states "through historic IP resolution overlap between the same domains alternately resolving to either the 223.25.233[.]248 or 196.45.144[.]12.   This shifting of IP resolutions back and forth indicates Nitro is in control of these domains."[106]

Carbanak Malware

A paper released by Trustwave in November 2016 included malware hashes in the IOCs that were part of the Carbanak malware.[107] [108]   There were four Webzilla B.V. owned IP addresses that supported the malware associated to that hash based on VirusTotal Intelligence **(78.140.136[.]87, 88.85.84[.]98, 78.140.142[.]179, and 78.140.136[.]87)**.[109]   The malware supported by the Webzilla B.V. owned IP addresses is a sub program used to issue "update" commands to the primary Carbanak malware.   This version of the Carbanak malware supported an advanced attack methodology carried out by actors targeting three separate victims in the hospitality and restaurant industries.   Carbanak is a prolific crime group, well known for stealing over one billion dollars from banks in 2015 and more recently orchestrating an attack on the Oracle Micros Point of Sale(POS) support site that put over one million POS systems at risk.[110]

Statements from Deposition Testimony

Statements made during the deposition support that Root S.A., and XBT as an organization, do not actively prevent the use of their infrastructure to support malicious cyber activity.

Based on the review of the deposition testimony of Konstantin Bezruchenko, CTO of XBT, and Marc Goederich, Managing Director of Root S.A, it is not clearly evident that XBT has an adequate enterprise infrastructure monitoring in place or a formally defined procedure to investigate abuse notifications or references to XBT-owned infrastructure identified in government and private security reports on high profile cyber campaigns.

---

103 Palo Alto Networks, Inc. is a network and enterprise security company based in Santa Clara, California.
104 https://stat.ripe.net/widget/routing-history#w.resource=223.25.233.248
105 Refer to Exhibit 23.
106 https://app.box.com/s/drb0p2idherjlxlwdqh0nharpt310s8u (Exhibit 24).
107 Hash: 2937013f2181810606b2a799b05bda2849f3e369a20982a4138f0e0a55984ce4
108 Trustwave Holdings is an information security company that provides threat, vulnerability and compliance management services and technologies.
109 https://stat.ripe.net/widget/routing-history#w.resource=78.140.136.87; https://stat.ripe.net/widget/routing-history#w.resource=88.85.84.98; https://stat.ripe.net/widget/routing-history#w.resource=78.140.142.179; https://stat.ripe.net/widget/routing-history#w.resource=78.140.136.87
110 https://app.box.com/s/cbclbgiu54ihivxe7bvblwsv1e8jq44h (Exhibit 25).

Konstantin Bezruchenko Deposition

Based on our review of Bezruchenko's deposition and our experience working with other web hosting and network solution providers, it appears XBT's investigative and takedown process of malicious activity is inadequate when compared to processes followed by other companies. Additionally, in our experience it's unusual that the CTO would not have basic information regarding customer allocation.

- Bezruchenko repeatedly states that he does not know about server and resource distribution across the XBT platform. Those are unusual statements considering that he stated that he is partially responsible for entering into lease agreements for technology procurement.[111] An organization leveraging this many servers normally has a formally defined and communicated strategy for capacity planning and resource allocation. This is also supported by his statement that it takes "an enormous amount of time" to deploy Webzilla servers.[112]

- Bezruchenko states you "can't have" a PCAP file, even for a short period of time.[113] [114] Based on our experience, web hosting companies do maintain PCAP files for a period of time. Additionally, Bezruchenko emailed Goederich about the Grizzly Steppe report and asked, "I'm wondering if someone had visited data center to gain access to those servers, copy data, and install any wiretap devices to listen to Internet data towards this servers, et cetera."[115] Listening to Internet data requires access to PCAP logs, which indicates that Root S.A. does maintain them.

- Minimal information was provided about what the duty engineer does when he "tries to understand what is going on" when attacks are observed originating from a managed server.[116] In our experience, it is best practice for companies to have robust procedures around investigating attacks originating from the network, including documentation and review by management.

- Based on our experience, the customer onboarding and background check process seems ad-hoc, immature, subject to personal bias, or any combination thereof. Bezruchenko states that the background check is a factor when considering larger clients.[117] However, when discussing the Methbot client requesting 1,000 servers he contradicts this statement, testifying: "I knew he runs this company. That's all I know."[118]

- Bezruchenko does not know how many customers have been terminated as a result of violating the acceptable use policy of XBT. In our experience this is a highly unusual statement and is information that the CTO should know.[119]

---

111 Bezruchenko Dep. 32:21.
112 Bezruchenko Dep. 26:16.
113 Bezruchenko Dep. 173:3 - 173:8.
114 PCAP (packet capture) consists of an application programming interface (API) for capturing network traffic.
115 Bezruchenko Dep. 261:4.
116 Bezruchenko Dep. 75:4.
117 Bezruchenko Dep. 81:9.
118 Bezruchenko Dep. 225:11.
119 Bezruchenko Dep. 106:14.

- Bezruchenko notes that Root S.A. was in the "business of -- I have called -- cheap dedicated servers" and that XBT wanted to enter the business.[120] In our experience, organizations that run cheap dedicated servers are resources for cybercriminals to launch malicious cyber attacks.

Marc Goederich Deposition

In general, Root S.A. does not appear to have any enterprise infrastructure monitoring in place to identify the use of their infrastructure to launch a cyber attack. Additionally, no formal procedures appear to be in place to monitor abuse alerts.

- Goederich states that there are no policies or procedures for governing ASNs and that they are governed based on "internal knowledge."[121] Based on our experience, its best practice for a web hosting company to define formal policies around the administration and maintenance of ASNs.

- When investigating IPs or customers Goederich indicates they place reliance on Googling their own IP addresses and ASNs to see what information is reported or "if anything bad is happens."[122] Goederich also indicates they do check Spamhaus, but in our experience it's a best practice for an ISP to have an automated process to collect or query key data about a specific server.[123]

- Goederich states that the company monitors the rate limit of outgoing emails but does not monitor them for malware or phishing attacks because he is "not allowed by Luxembourgish law".[124] This statement is confusing and unusual. It's unclear from our experience and research why Root S.A. cannot monitor outbound email traffic for the purposes of detecting phishing attacks.

- Goederich states that, to his knowledge, Root S.A. does not have any measures in place to prevent data abuse or hacks on its infrastructure.[125] Based on our experience, this is a highly unusual statement because it is a best practice that web hosting companies have policies in place to restrict the launch of malicious attacks on their infrastructure.

- Goederich states there is no employee or individual at Root S.A. responsible for ongoing security review at Root S.A.[126] Based on our experience, it is not a best practice for a web based technology firm to not have a dedicated resource responsible for network security.

- Goederich stated that Root S.A. is not ISO certified because of "time, costs, and other customers didn't demand it."[127] This is a highly unusual statement because web hosting companies typically advertise their level of security as a feature of its infrastructure.   Bezruchenko's deposition identified Amazon Web Services (AWS) as a competitor and AWS advertises ISO compliance.[128] [129]

---

120 Bezruchenko Dep. 143:4
121 Goederich Dep. 24:1.
122 Goederich Dep. 24:6.
123 Goederich Dep. ibid
124 Goederich Dep. 52:14 – 54:25.
125 Goederich Dep. 75:2.
126 Goederich Dep. 83:16.
127 Goederich Dep. 84:12.
128 https://aws.amazon.com/compliance/iso-27001-faqs/

- Goederich confirms that no internal investigation was launched after he was contacted by the local authorities about an IP address listed on the Grizzly Steppe report.[130]

- Goederich confirms that he has received over 400,000 abuse notifications over the past seven years but cannot comment on whether or not they were all checked.[131]   Based on our experience, not knowing how many abuse notifications were investigated is an abnormal practice and further illustrates that XBT does not apparently care what activity is originating from their network. Our experience is that web hosting companies have automated work flows so that all abuse notifications are reviewed and closed.

Based on this deposition, TOR Exit notes and services are used on Root S.A. infrastructure, and it had been brought to their attention multiple times by law enforcement and through abuse notifications.[132]   TOR networks can be used to anonymize illegal activities, such as buying and selling of drugs. These networks can also be vectors for cyber attacks.[133]   Goederich stated in testimony that he does not know that "TOR networks anonymizes" its users, which is a confusing statement given his response to law enforcement when contacted about an IP address in the Grizzly Steppe.[134]   Analysis performed by private security firm HackTarget showed that in 2013 Root S.A. has the second highest concentration of Tor Exit nodes for Internet Providers based on the ASN netblock.[135] [136]

Public Reputation Related to Malicious Cyber Activity

In addition to directly providing web-hosting services, XBT appears to lease sections of their infrastructure to other web-hosting companies. Many of these lessee companies are reportedly tied to malicious cyber activity. FTI reviewed approximately 75 entities either owned by XBT or using ASNs owned by XBT in order to identify adverse information, including whether XBT customers were named as conduits for malware or malicious or criminal cyber activity. FTI found credible sources naming XBT affiliates as being involved in adverse, malicious or criminal activity. Those entities included companies owned by XBT (e.g. Webzilla) and companies that lease technical infrastructure from XBT (e.g., McHost and CubeHost). FTI also identified reporting on Internet technology blogs and other similar outlets that cited entities leasing IP blocks owned by XBT as supporting malicious cyber activity.

---

129 Bezruchenko Dep. 54:6.
130 Goederich Dep. 160:1.
131 Goederich Dep. 227:2 – 227:12.
132 Goederich Dep. 157:14,22,25 158:5 159:2,3,11 163:14 164:1,14,18 165:5,14,15,21 166:8,14,16,23 167:4,8 182:15 -
183:191:2,6,19,25 192:7,9 207:22,25208:10 218:12 219:15 220:8,10,14,25 221:3,7 230:19.
133 https://www.recordedfuture.com/monitoring-tor-exit-nodes/
134 Goederich Dep. 167: 1.
135 https://hackertarget.com/tor-exit-node-visualization/
136 Use open source tools and network intelligence to help organizations with attack surface discovery and identification of security vulnerabilities.

Entity	Entity Type	Adverse High Level Summary
1-800-HOSTING, Inc. ("1-800-Hosting"), now Webzilla Dallas, Inc. (XBT)	Web hosting	Cited in August 2008 by the *Dallas Morning News* as a **company under investigation by the Russian government for hosting websites linked to two Russian cyber criminals**.[137] The Russian government reportedly sought assistance from U.S. Secret Service officials in Dallas in obtaining additional information on 1-800-Hosting. Specifically, Russian authorities reportedly were investigating allegations the company hosted websites controlled by Russian citizens Ivanin Maxim Andreevich and Krasov Alexander Igorevich, who reportedly embedded viruses on websites used to capture and exploit victim banking information.[138] The *Dallas Morning News* appears to be the sole media outlet that covered this investigation and its outcome is unknown.[139] Cited in a February 2008 report by Shadowserver Foundation ("Shadowserver"), a non-profit volunteer organization that gathers, tracks and reports on malicious software, botnet activity and electronic fraud.[140] Shadowserver reportedly reviewed 80 domain names associated with spyware, phishing and other malicious activity and suggested further investigation into 1-800 Hosting's ASNs.[141] It is unclear whether Shadowserver pursued any additional investigation into 1-800-Hosting. **FTI notes this activity pre-dates XBT's acquisition of 1-800-Hosting. XBT acquired the company in November 2012.**[142]
Fozzy Inc. (XBT)	Web hosting	According to the *McClatchy DC Bureau,* fozzy.com is a site **"used to heavily host pornography."**[143]
WZ Communications Inc. (XBT)	Web hosting	Named in six Host Exploit "Top 50 Bad Hosts" reports between 2010 and 2012 as a **botnet command-and-control server**.[144] Consecutively ranked #15, #26, #30 and #31 on Host Exploit's list of Top 50 hosting companies with highest observed concentrations of malicious activity.[145]
Webazilla (XBT)	Web hosting	Named in Host Exploit "World Hosts Report" in March 2014 as **hosting Zeus botnets**.[146] Cited by Dutch reporter Karen Spaink in February 2008 as **hosting child pornography**. Spaink examined several Dutch websites on the National Police Forces blacklist and found that almost all the sites were openly hosted through two providers, Webazilla and Leaseweb. According to

---

137 "The Dallas-Russia axis of evil online fraud (allegedly)," DallasNews.com, August 11, 2008.
138 Ibid.
139 DallasNews.com is the online website for the Dallas Morning News newspaper.
140 https://www.shadowserver.org
141 www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf
142 http://www.marketwired.com/press-release/xbt-holding-ltd-acquires-1-800-hosting-inc-1724402.htm 1/
143 www.mcclatchydc.com/news/nation-world/national/article125910774.html
144 http://hostexploit.com/?p=reports
145 Ibid.
146 Ibid.

Entity	Entity Type	Adverse High Level Summary
		the KLPD both Webazilla and Leaseweb hosted child pornography.[147]
Webzilla (XBT)	Web hosting	Cited in a March 2016 report submitted to the U.S. Copyright Office Library of Congress regarding music pirating and violations of the Digital Millennium Copyright Act ("DMCA").[148] In the report, Webzilla is cited as a hosting company **refusing to terminate service with their customers despite receiving thousands of notices of infringement attributable to their subscribers' accounts.**[149]
McHOST (customer)	Web hosting	According to *TrendLabs Security Intelligence Blog*, McHost is a Russian web-hosting company that is purportedly **"very friendly with Russian/Ukrainian cyber criminals" and described as a "criminal haven for Russian/Ukrainian cyber criminals."**[150]
CUBEHOST (customer)	Unknown, likely web hosting	Named in a *Krebs on Security* article as a dormant site registered to Artem Tveritinov, CEO of Infocube, an anti-virus information security company that is allegedly a "minor partner" of Kaspersky Labs. **The phone numbers listed in the domain name registration for cubehost.biz are two Chinese phone numbers traced back to other domains seen launching malware**. Tveritinov's company is also accused of spreading malicious software used to steal banking information.[151]
Colo4, LLC (customer)	Colocation/Cloud Computing	Named in a *Krebs on Security* article as **one of numerous companies with networks "shown to have been phoning home to some of the same control infrastructure that was used in RSA attack."**[152] FTI notes that several large companies are on the list, including Motorola, eBay, IBM, Research in Motion, and that not every company on the list may be culpable.

Host Exploit Reports

FTI also reviewed all Host Exploit "Top-50 Bad Hosts and Networks" reports published online from December 2010 to March 2014 that rank web-hosting companies by concentration of malicious activity.[153] **XBT subsidiaries Webazilla, Webazilla BV and WZ Communications are cited in these reports as known hosts of malicious activity; operators of botnet and command-and-control servers; and hosts of high levels of Zeus botnet activity.**[154] [155]   Between 2010 and 2012, WZ Communications ranked between 15 and

---

147 "Child pornography: fight it or hide it?" Het Parool, February 19, 2008.
148 https://www.riaa.com/wp-content/uploads/2016/03/Music-Community-Submission-in-re-DMCA-512-FINAL-7559445.pdf
149 Ibid.
150 http://blog.trendmicro.com/trendlabs-security-intelligence/unscrupulous-russian-cyber-criminals-attempt-to-capitalize-on-grisly-death/

153 http://hostexploit.com/?p=reports. Note that Host Exploit only published reports from December 2010 and March 2014 online. It is unclear if there are additional reports that pre-date or post-date these reports.
154 "A form of botnet delivered via a Trojan payload. Zeus has been continually improved, with its many variations proving to be adept at bypassing security systems and gathering large networks of zombie machines," per Host Exploit.

31 on Host Exploit's list of Top-50 "bad" hosting companies and was cited as a command-and-control server for malicious botnets. Hosting companies are ranked by the concentration of malicious activity, or what Host Exploit refers to as the "HE Index."[156] The HE Index is the organization's method of assigning a value to the reputations of Autonomous Systems linked to cybercrime. **Host Exploit reportedly was one of the first organizations to highlight 2008 Russian cyber attacks on the nation of Georgia and also to expose cybercriminal webhosts McColo and EstDomains.**[157]

Based on FTI's analysis of all available Host Exploit reports, the following negative information was developed for Webazilla and WZ Communications:

Report Year/Edition	XBT entity	Top 50 "Bad Host" HE Ranking (out of 50)	Country	IPs	Cited as Botnet command-and-control Server (Y/N)	Cited as Zeus Botnets (Y/N)
World Hosts Report March 2014	Webazilla B.V.	#29	Netherlands	77,056	N	Y
Top 50 Bad Hosts and Networks 2nd Quarter 2012	Webazilla	#21	Cyprus	63,488	N	N
Top 50 Bad Hosts and Networks 1st Quarter 2012	WZ Communicat ions Inc.	#15	U.S.	13,056	Y	N
Top 50 Bad Hosts and Networks 1st Quarter 2012	Webazilla	#28	Ukraine	61,440	N	N
Top 50 Bad Hosts and Networks 4th Quarter 2011	WZ Communicat ions Inc.	#30	U.S.	9,216	Y	N
Top 50 Bad Hosts and Networks	WZ Communicat ions Inc.	#26	U.S.	9,216	Y	N

---

155 The Webazilla infrastructure (including ASN) was rolled into the Webzilla infrastructure in 2010. To date, public IP registration information still references the entity as "Webazilla."
156 http://hostexploit.com/?p=report. Host Exploit is an open-source community and non-profit organization dedicated to cybercrime research with a focus on hosts and registrars.
157 http://hostexploit.com/

Report Year/Edition	XBT entity	Top 50 "Bad Host" HE Ranking (out of 50)	Country	IPs	Cited as Botnet command-and-control Server (Y/N)	Cited as Zeus Botnets (Y/N)
3rd Quarter 2011						
Top 50 Bad Hosts and Networks 2nd Quarter 2011	WZ Communications Inc.	#31	U.S.	8,960	Y	N
Top 50 Bad Hosts and Networks 1st Quarter 2011	WZ Communications Inc.	N/A	U.S.	8,960	Y	N
Top 50 Bad Hosts and Networks 4th Quarter 2010	WZ Communications Inc.	N/A	U.S.	7,936	Y	N

Conclusions

XBT and its affiliated web hosting companies have provided gateways to the internet for cybercriminals and Russian state sponsored actors to launch and control large scale malware campaigns over the past decade.[158]

Data provided by Bitly indicates that an XBT affiliate owned infrastructure was used to support the malicious spear phishing attack of Democratic Party leadership in 2016 which resulted in the theft and subsequent publication of highly sensitive information related to the Hillary Clinton presidential campaign.
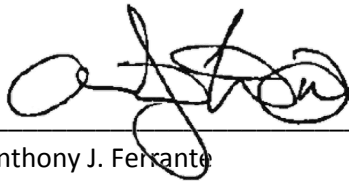
Technical analysis of XBT infrastructure and U.S. government issued reports on Russian cyber espionage tactics indicates that IP addresses owned by XBT were utilized by Russian civilian and military intelligence services (RIS) to compromise and exploit networks and endpoints associated with the 2016 U.S. election. Additionally, evidence suggests that COZY BEAR and FANCY BEAR, the Russian government affiliated APT groups responsible for hacking the Democratic Party leadership, have used XBT infrastructure to support other malicious activity.

Reputable private security firms have listed XBT infrastructure in a number of independent reports relating to high profile malware campaigns, including attacks by Russian state actors. Those reports suggest XBT infrastructure has been used to propagate malware, to attack the Ukrainian power grid, to engage in spear phishing attacks, to deliver ransomware, to launch online advertising click-fraud theft schemes, and to host botnets. Additionally, XBT has a public reputation for hosting malicious cyber activity. Media research evidences multiple affiliates as being involved in adverse, malicious or criminal activity. More specifically, XBT subsidiaries Webazilla, Webazilla BV and WZ Communications are cited in reputable publications as known hosts of malicious activity; operators of botnet and command-and-control servers; and hosts of high levels of Zeus botnet activity.

---

158 Refer to Exhibit 25

FTI's findings illustrate a pattern that XBT infrastructure has been a resource for cybercriminals to launch attacks without fear of repercussion, including specifically cybercriminals engaging in Russian state sponsored malicious activities. Based on documentation produced during discovery and deposition transcripts, Gubarev and other XBT executives do not appear to actively prevent cybercriminals from using their infrastructure. Minimal, if any, investigations were performed by XBT when their infrastructure was cited in high profile government or private security firm reports. For example, the first email correspondence from XBT executives about the Root. S.A owned IP addresses noted in the Grizzly Steppe report was sent in September 2017, almost nine months after the report was published.

Executed on the 25th day of May, 2018.

_____

Anthony J. Ferrante
Senior Managing Director, Global Head of Cybersecurity
FTI Consulting, Inc.

Overview of Exhibits

Exhibit ID	Exhibit Description
Exhibit 1	Curriculum vitae of Anthony J. Ferrante
Exhibit 2	ASN Overview Technical Support
Exhibit 3	CrowdStrike Report: Bears in the Midst: Intrusion into the Democratic National Committee
Exhibit 4	Bitly WarRoom Presentation about Democratic Party Spear Phishing Attack
Exhibit 5	Bitly Audit Log Data
Exhibit 6	Technical Evidence to support the SSL Connection
Exhibit 7	JAR-16-20296A - GRIZZLY STEPPE – Russian Malicious Cyber Activity and Published IOCs
Exhibit 8	Grizzly Steppe Technical Support
Exhibit 9	WhiteOps Report: The Methbot Operation
Exhibit 10	Methbot IOCs Published by Methbot
Exhibit 11	ICS-ALERT-17-206-01 - CRASHOVERRIDE Malware
Exhibit 12	ESET Report: WIN32/INDUSTROYER - A new threat for industrial control systems
Exhibit 13	F-Secure Report: COSMICDUKE Cosmu with a twist of MiniDuke
Exhibit 14	Kaspersky Lab Report: Unveiling "Careto"-The Masked APT
Exhibit 15	ESET Report: OPERATION POTAO EXPRESS - Analysis of a Cyber-Espionage Toolkit
Exhibit 16	Sedreco Technical Connections
Exhibit 17	ESET Report: En Route with Sednit
Exhibit 18	Swiss Government Computer Emergency Response Team (i.e. Gozi)
Exhibit 19	Cisco Talos Report: Rigging compromise - RIG Exploit Kit
Exhibit 20	Damballa Report: PonyUp - Tracing Pony's Threat Cycle and Multi-Stage Infection Chain
Exhibit 21	Kaspersky Lab Report: DarkHotel Indicators of Compromise
Exhibit 22	DarkHotel Technical Connections
Exhibit 23	Nitro Technical Connections
Exhibit 24	Palo Alto Networks Report: New Indicators of Compromise for APT Group Nitro Uncovered
Exhibit 25	Trustwave Report: New Carbanak / Anunak Attack Methodology
Exhibit 26	XBT Timeline of Malicious Cyber Activity
Exhibit 27	Dragos Report: CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations