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 Dr. Eric Cole
On behalf of the plaintiffs

1. Introduction

1. I, Dr. Eric B. Cole, have been retained as a technical expert on behalf of the plaintiffs, in connection with the above-captioned defamation in case, in which the defendants made false and inaccurate statements regarding the plaintiffs. Specifically, regarding the statement: *"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."*

2. Experience and Qualifications

a) Curriculum Vitae

2. I hold a master's degree in computer science and a doctorate in information security and have worked in the cyber and technical information security industry for over 25 years. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

3. The details of my education are summarized in my curriculum vitae ("CV") attached hereto as Appendix A of this Report.

4. I am the founder of Secure Anchor Consulting where I provide cyber security consulting services and lead research and development initiatives to advance information systems security. I am a Fellow and instructor with The SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses such as SEC401-Security Essentials and SEC501-Enterprise Defender.

5. I have worked for the government for 8 years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have

held various top-secret security clearances with Department of Defense (DOD), CIA, and Nuclear Regulatory Commission (NRC). I have worked for a wide range of government organizations including FBI, National Security Agency, CIA, Department of Energy, DOD, the Treasury, Secret Service and the NRC.

6. While serving as a Senior Officer for the Central Intelligence Agency as Program Manager / Technical Director for the Internet Program Team with Office of Technical Services, I implemented the Internet Program Team that designs, develops, tests, and deploys internet security products in 3 to 6 month intervals. In this role I received a letter of appreciation from the DCI (Director Central Intelligence) and six Exceptional Performance Awards.

7. As a member of the Information Security Assessment Team with the Office of Security I also evaluated and performed security assessment of network operating systems to identify potential vulnerabilities and solutions. I also designed a large-scale auditing system with automated review capability and worked on several virus investigations for the Office of Security.

8. In my role as Chief Information Officer for the American Institutes for Research, I have repaired and developed IT infrastructures for various organizations and provided technical support for the Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defense responsible for the development of new technologies for use by the military.

9. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as technical advisor in high-profile security projects for government clients including the Department of Defense, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

10. As Chief Technical Officer for McAfee I executed the technology strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity I worked closely with groups tasked with the development of intellectual property.

11. The details of my work experience and research are summarized in my CV attached hereto as Appendix A of this Report.

12. I am a contributing author of "Securing Cyberspace for the 44th President." and served as a commissioner on cyber security for President Obama. My 8 books on cyber security include "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. I have also written several articles that have been published.

13. In my past and current roles, I am actively involved in evaluating cyber security incidents and performing analysis on overall cyber security matters, to include networking and how the Internet works and operates.

14. The details of my publications, including those I have authored within the last 10 years, are summarized in Appendix A.

b) Prior Testimony

15. A list of cases in which I have testified at deposition or trial or in written reports during at least the past five years is attached as Appendix A of this Report.

c) Compensation

16. My rate of compensation for my work in this case is $550 per hour plus any direct expenses incurred. My compensation is based solely on the amount of time that I devote to activity related to this case and is in no way affected by any opinions that I render. I receive no other compensation from work on this action. My compensation is not dependent on the outcome of this matter.

3. Materials Considered

17. My opinions, expressed herein, are based on information I have reviewed to date including the materials referenced herein and the expert report of Anthony J. Ferrante from FTI Consulting, Inc. My opinions are based on my knowledge and experience in the fields of computer and network security, networking and overall knowledge of the Internet.

4. Summary of Opinions

18. After studying the materials listed in Section 3 of this Declaration, I reached the conclusions discussed herein. It is my opinion that the defendants had no factual information or proof to support the claims made against the plaintiffs. The claims made including the statement: *"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."* has no factual backing, are unfounded, and there is no supporting evidence that backs this or any other claims.

19. In addition, I have found that Anthony J. Ferrante's expert report lacks accuracy and forensic soundness, and does not provide any supporting evidence to back the statements made by the defendants. Actually, to the contrary, Mr. Ferrante's export report supports the conclusion that there is no actual supporting evidence. For example, on page 13 of his report, he states: "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." This theme of failing to provide any foundation is a theme throughout Mr. Ferrante's report.

20. It is important to note the word "suggests" was used 4 times in the Executive Summary (9 times total in the report) to describe specific "findings" that had no definitive evidence or proof and the word "support" was used two times to describe technical functions that are normal in any ISP environment and have no relevance to actual actions taken by plaintiffs. In addition, the FTI report never

once uses the words "prove" "proves" or "proof" and uses the term "forensic" only in reference to forensic accounting in the Qualifications section.

21. In his report, Mr. Ferrante states that 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.

22. Other than inaccurate and unsupported opinions, Mr. Ferrante does not provide any actual proof to support any of the above statements. The only analysis Mr. Ferrante performed is an analysis of IP addresses, which contain no proof that an entity actually engaged in any wrong doing. IP addresses of many large companies have been used in attacks, unbeknownst to the company that owns the IP address. As will be shown in my report, stating that an IP is associated with a company is not direct correlation that the company was deliberately and maliciously involved in the activity. This continuous false analysis made by Mr. Ferrante either demonstrates his lack of knowledge of cyber-attacks or his creativity in trying to stretch the truth beyond any factual proof.

23. The analysis performed by Mr. Ferrante, not only provides no factual proof that the *plaintiffs* did anything malicious or engaged in any wrongdoing, but Mr. Ferrante's analysis would be true for any ISP or company, and, indeed, would even be true for Buzzfeed. IP addresses are often spoofed and organizations, including ISPs, very often have systems that are compromised by an adversary and used for an attack, completely unbeknownst to the organization. It is important to note that the NSA report

referenced by Mr. Ferrante lists thousands of IP addresses, of which XBT address are only a tiny fraction of a percent. According to BuzzFeed's logic, all owners of these thousands of addresses are complicit. So why aren't other IP address holders accused?

24. It is important to point out that XBT and other similar service providers networks transmit over 500 Gbit/s of data (equivalent of 13+ DVD disks) per second. Storing and processing this data is extremely expensive and not feasible for any ISP.

5. Introduction: Technical Inaccuracies

25. FTI's Investigative Findings begins with a misleading and technically inaccurate analogy in the Background and Approach section. This analogy systematically excludes critical components of the Internet and incorrectly shapes the narrative, while all but invalidating the approach of FTI's technical investigation.

26. The technical descriptions that were offered are at best partially accurate and framed in such a way as to overstate XBT's capabilities and influence in the process of botnet use and virus delivery. Before comparing the Internet *"in terms of old-fashioned mail delivery"* it is important to first correct the technical inaccuracies described by Mr. Ferrante in this report.

27. First, Mr. Ferrante stated: "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." In this statement there is a glaring technical inaccuracy that no expert witness who has "extensive practical expertise researching, designing, developing, and hacking complex technical applications and hardware systems" should ever make. There are two ways to read this misleading sentence due to the way it has been structured. Neither is completely accurate and regardless of how the reader interprets it, but most notably it clearly attempts to shape the narrative to a skewed view of how the Internet actually works.

28. "IP addresses are unique numbers assigned to all individual parts of the Internet – the lines of communication over which online information flows…." Read one way, this statement describes the Internet as "the lines of communication over which online information flows". This is not correct. The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. The other way to read it implies IP addresses are responsible for information passing across the Internet. This is also not correct. An IP address serves two principal functions: host or network interface identification and location addressing. In short, IP addresses ARE NOT the lines of communication over which online information flows. The lines of communication are just that. Lines. Most commonly taking the form of fiber optic cables. In my expert option, to include such a glaring technical error between two technically correct statements, shows a desire to mislead a non-technical reader.

29. That opinion is immediately reinforced by the very next sentence in this portion of the report. Mr. Ferrante, on page 9, states: "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." Like the first sentence Mr. Ferrante uses a glaring technical inaccuracy mixed in with some technically correct information. Autonomous Systems ARE NOT the backbone of the Internet. The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA) and by five regional Internet registries (RIRs). An RIR is an organization that manages the allocation of Internet number resources within a particular region of the world. Internet number resources include autonomous system (AS) number and IP addresses which are assigned by the RIR to end users and local internet registries, such as Internet service providers. Describing an

Autonomous System this way frames an analogy that is not only misleading, but also reveals a fundamental lack of understanding of the most basic mechanics of the Internet.

30. For purposes of continuity I will continue to use Mr. Ferrante's analogy "to think of the Internet in terms of old-fashioned mail delivery" but in a technically accurate manner. For an old-fashioned mail delivery system to work four basic, and necessary, components are required.

- A sender
- A receiver / destination address
- A mail transportation service which supports a specific region such as a town or city.
- A medium for moving the mail from one location to another by the use of an interstate highway or flight route.

31. Translating these components into their digital equivalent appears as follows:

- A sender – in this example an individual or group specifically wishing to transmit information ranging from a document to a photo to a virus.
- A receiver / destination address – this is the IP address, the specific identifier that ensures the digital information arrives at the correct computer.
- A mail transportation service – in this example that service could be XBT/Webzilla who provides "mail delivery" for a certain region.
- A medium for moving the mail – this is the actual backbone of the Internet, which are the data routes that connect large, strategically interconnected computer networks and core routers globally. Companies such as AT&T, Verizon, Sprint, and CenturyLink own some of the largest Internet backbone networks and sell their services to Internet Service Providers such as XBT/Webzilla.

32. With these clarifications in place it quickly becomes clear that Mr. Ferrante is systematically ignoring the transportation component of the Internet by incorrectly describing IP addresses as *"the lines of communication over which online information flows"* which is the equivalent of saying a home address is how mail moves across the country and that *"Autonomous Systems are the backbone of the Internet"* which is the equivalent of saying a regional post office that services a city is the national highway system.

33. Obviously, anyone who has ever sent a letter knows that just having a home address doesn't get a letter to a destination and that the local post office isn't an interstate highway or air route. In addition, anyone who has sent or received a letter knows that the return address provides no confirmation of the actual sender of a letter. In sending a letter, you can write in anyone's address as the return address and there is no validation performed. Similarly, on the Internet, IP addresses can easily be spoofed or modified.

34. This leads us to the real heart of the matter, and a critically important question to ask, and answer, using the correct framework of this analogy: Is a local post office liable for the <u>intent and content</u> of the mail it transports out of the neighborhood as part of its service?

35. To ask this question in the digital realm; is Webzilla/XBT, and the autonomous system it operates, which provides a service as an access point to the larger Internet responsible for the data that passes over its infrastructure? Autonomous Systems are issued regionally by Regional Internet Registries (RIRs), which receive blocks of autonomous system numbers to hand out from the Internet Assigned Numbers Authority (IANA). To be part of the Internet, an autonomous system connects to at least one other network and they exchange network information with each other. What responsibility does the RIR have in the transmission of data?

36. To expand on this point, why aren't companies such as AT&T, Verizon, Sprint, and CenturyLink which own the Internet backbones also being held accountable in this report for the services they sell to Webzilla? It could also be brought into question, based on the logic of this report, why the

autonomous system on the receiving end is also not being held accountable for the final steps in transmission of botnets and porn traffic to transmit viruses, plant bugs, steal data and conduct 'altering operations' to the Democratic party leadership.

37. Mr. Ferrante also makes an unsupported claim that XBT has poor security practices. In his executive summary, Mr. Ferrante states: "Depositions of key XBT executives and a review of communications produced show that XBT does not have an adequate enterprise infrastructure monitoring process…". However, Mr. Ferrante fails to provide any of the depositions, communications, or any other factual information to support this claim. While there is zero proof in his report that this is true, even if it was, it is irrelevant to this case. Buzzfeed did not accuse Webzilla of having poor security practices and vetting procedures, they accused "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."

38. . Buzzfeed could have easily claimed that Seagate was at fault because viruses were stored on their hard drives or that Microsoft was at fault because a virus targeted a Windows operating system.

39. Mr. Ferrante also stated in his report that Webzilla is on a list of alleged "bad actors." However, there are other companies on the list, such as GoDaddy and Google, which means it is not uncommon for legitimate companies to appear on the list, especially if they are an ISP.

40. XBT/Webzilla is not responsible for every bit of data that a bad actor passes over its infrastructure any more than a post office is responsible for the actions of the Unabomber.

41. It is therefore false and defamatory for Buzzfeed to make a blanket statement that the plaintiffs are using botnets and porn traffic to transmit viruses, plant bugs, steal data and conduct 'altering operations' against the Democratic Party leadership. XBT/Webzilla enables the transmission of data, but so does every other autonomous system on the planet. XBT/Webzilla also ENABLES the successful transmission of millions of legitimate emails and files every day.

6. Key Point: What BuzzFeed is accusing XBT of is a global challenge that all ISP's face

42. Excerpt from the "Conclusions" section of the FTI report: 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. Mr. Ferrante fails to state that this is true for every ISP and is not unique to XBT/Webzilla.

43. The FTI report, in reality, is little more than a cobbled together set of random analysis with no conclusive evidence that supports the claims they are defending. To avoid unnecessary repetition by addressing each point made in the report I have summarized a list of some of the largest cyber-attacks in history having come from different parts of the world, specifically different Regional Internet Registries (RIRs) and the Autonomous Systems (AS) which belong to those regions. The purpose of these examples is to illustrate that bad actors use Autonomous Systems (AS) all over the world and that the ASs and ISPs whose infrastructure were used to carry out these attacks were not singled out or accused by the victims as the perpetrators of these events simply because the data passed across the systems they managed.

44. Additionally, the increased use of encryption on the Web is a substantial privacy improvement for users. When a web site does use HTTPS, an ISP cannot see URLs and content in unencrypted form.

45. It is common practice for ISP users to utilize virtual private network (VPN) tools which reduces what an ISP is able to see down to the VPN itself, timing and amount of data sent. No other insights as to what is being transmitted is visible. This reality only amplifies the monitoring and analysis challenges for an ISP even with the assumption it had the ability to process the sheer volumes of traffic that pass through its systems.

46. To further emphasize the challenge all ISPs have with respect to malicious traffic, please see the highlighted sections in the articles quoted below:

Title: **ISPs 'should be responsible' for hacker attacks**

Source: Daily news

Date: 9 November 2006

https://www.newscientist.com/article/dn10494-isps-should-be-responsible-for-hacker-attacks/

The idea of requiring ISPs to guard against DoS attacks will be strongly resisted by the companies concerned, says Malcolm Hutty of the London Internet Exchange, an association of London-based Internet providers. "That idea is guaranteed to fail," he says. "It's not the ISP's fault that DoS attacks happen – it is the computer's fault for allowing the bots to be planted."

Distinguishing between malicious and innocent traffic would also be too time-consuming and expensive, Hutty contends, and would cause delays for users too.

"Recognizing DoS attacks is not easy," Hutty says. He notes that the public blog of the Internet Governance Forum, an event in Athens, Greece, last week was so popular that its servers went down. "That was not a DoS attack," Hutty says, "but it looked like one. How is the ISP to know that it is not genuine site popularity, rather than some nefarious purpose?"

Ollie Whitehouse of antivirus firm Symantec in the UK says criminals could begin encrypting their attack commands if ISPs start inspecting every packet they handle. "That will make spotting a DoS attack a whole lot harder for an ISP," he says. Hutty agrees: "If we try to tell the good traffic from the bad, it'll only incentivise the bad guys to make it more indistinguishable."

Harnessing deep packet inspection is already a politically charged issue. ISPs could use the technique to create a multi-tiered Internet, offering different download speeds or quality of service to different users, and infringing the principle of "net neutrality"

Title: **Amid cyberattacks, ISPs try to clean up the Internet**

Source: Michael Kan, U.S. Correspondent, IDG News Service

Date: Feb 23, 2017

The tracking capabilities of Level 3 highlight how Internet service providers can spot malicious patterns of activity over the Internet, and even pinpoint the IP addresses that are being used for cybercrime.

In more extreme cases, Level 3 can essentially block bad traffic from harassing victims, and effectively shut down or disrupt the hackers' attacks.

So why aren't ISPs doing more to crack down on cybercrime? The issue is that an ISP's ability to differentiate between normal and malicious Internet traffic has limits, and finding ways to properly respond can open a whole can of worms.

Malicious patterns

Level 3 has built up a database of 178 million IP addresses -- most of them static IP addresses -- that it has connected to suspected malicious activity. It's done so by pinpointing patterns that deviate from "known good" Internet traffic, Drew said. He compared it to running a post office. Although Level 3 isn't examining the content of the Internet traffic or the "envelopes" passing through, it does know who's sending what and to whom.

One might wonder why Level 3 doesn't just block these IP addresses from the Internet. But that can be problematic. Often, users of hacked computers are unaware their machines have been compromised, and it may be unclear whether some of those machines are also being used for important purposes, such as legitimate financial transactions.

Blocking those machines could potentially mean stopping millions of dollars in transactions, Drew said.

Instead, the company tries to notify the users of those IP addresses. In many cases, they are businesses, which can be quick to respond, Drew said. However, when it comes to consumers, there's no phonebook linking one person to an IP address.

Confronting the limits

Overall, it can be an uphill battle. "For every IP address we repair, more IP addresses are being compromised," Drew said.

Other ISPs, including some in Europe, have also been notifying customers when their machines might be infected. It's become a years-old, growing practice, but getting users to fix their infected computers isn't always straightforward, said Richard Clayton, a security researcher at the University of Cambridge and director of its cloud cybercrime center.

Even when ISPs send warning messages to users, what then? Not every PC user knows how to resolve a malware infection, Clayton said. For ISPs, it can also be a matter of cost.

> "Of course we want to see ISPs helping, but they are in a competitive market," he said. "They are trying to cut their costs wherever they can, and talking to customers and passing on a message is not a cheap thing to do."
>
> In addition, ISPs can't identify every malicious cyberattack. Most hacking attacks masquerade as normal traffic and even ISP detection methods can occasionally generate errors, Clayton said.
>
> "If you have a 99 percent detection rate, in an academic paper, that sounds fantastic," he said. "But that basically means one out of 100 times, you'll be plain wrong."
>
> No magic bullet
>
> That's why taking down suspected hackers usually requires collective action from law enforcement and security researchers who have thoroughly investigated a threat and confirmed that it is real. Governments and ISPs have also become involved in creating websites and services telling users how to effectively clean up their PCs.
>
> It's a difficult balancing act for ISPs, said Ed Cabrera, the chief cybersecurity officer at antivirus vendor Trend Micro. "They can do a lot of detection quite easily," he said. "But the blocking piece is not something that they want to take responsibility for."
>
> Cybercriminals are also continually elevating their game, making them harder to detect. "The problem is nowhere near black and white," Cabrera said. "We're quick to say ISPs aren't doing enough, but I think often times that's unfair."
>
> Level 3's Drew said it's tempting to think that the world's cybersecurity problems can be solved with a magic bullet. But for now, it will take a collective effort -- of ISPs, governments, businesses and consumers -- to clean up the Internet and secure today's devices.
>
> "Even if we were able to deploy exhaustive technology to analyze the bad, ugly traffic, it still doesn't fix the infected devices," Drew said. "The end user still has a role to properly patch that device."
>
> He also encourages all ISPs to take Level 3's approach and notify customers when their computers have been hijacked by hackers.
>
> If more ISPs did this, Drew said, "we might make a dent."

47. Looking closely at the information presented in Mr. Ferrante's report, the technical conclusions do show that specific IP addresses assigned to Webzilla did have traffic pass over them that

"suggested" certain types of behavior. What Mr. Ferrante is not saying in his conclusions, and what the previous examples have illustrated, is that this type of traffic passes across IPs in every AS across the world.

48. The explanation attempts to mislead by heavily suggesting that the events described in their investigation are 1) unique to Webzilla/XBT and 2) malicious with intent. Neither are true.

49. To refer back to Mr. Ferrante's analogy of an old fashioned mail system, his approach and limited information attempts to lead a reasonable person to conclude that the Webzilla/XBT post office is the only one that must receive and deliver mail from a neighborhood with bad actors and that because they are assigned a range of IP addresses from a larger governing body with this express intent of providing service to all that need it and that Webzilla/XBT is also somehow responsible for monitoring and stopping every malicious packet that traverses its network.

7. <u>Key Point: No forensic investigation was conducted.</u>

50. This investigation has no information based on collection and analysis from XBT Holding systems. No analysis of server logs and hard drives. No analysis of router logs. No email or other digital communication analysis to determine if XBT Holding had any operational plans to deploy botnets and distribute pornography with virus payloads to the Democratic party.

51. In addition, based on a list of IP addresses provided by the Democratic National Committee (attached hereto as Exhibit 1), listed below, none resolved to Webzilla. It is important to note that Amazon.com is on the list but not accused of malicious activity by the defendants.

176.31.112.10 – ISP: OVH SAS
46.165.208.108 – ISP: Leaseweb Deutschland GmbH
82.221.104.121 – ISP: Advania hf.
185.100.84.134 – ISP: Flokinet Ltd
58.49.58.58 – ISP: China Telecom Hubei
202.46.2.44 – ISP: IPTEKNET, Indonesian Science and Technology Network
185.86.148.227 – ISP: Makonix SIA
164.132.102.184 – ISP: OVH SAS
45.32.129.185 – ISP: Choopa, LLC

23.227.196.217 – ISP: Swiftway Communications
89.44.103.9 – ISP: UK Dedicated Servers Limited
52.74.169.204 – Amazon.com
218.1.98.203 – ISP: China Telecom
187.33.33.8 – ISP: Smart Solutions Comercio e Servicos Ltda
60.2.237.27 – ISP: China Unicom Hebei

8. Key Point: Assuming everything in the report were true, there is still no forensic evidence.

52. To avoid unnecessary repetition by addressing each point made in the report I am addressing the deficiencies and inaccuracies listed in the Executive Summary. First, it is important to note the word "suggests" was used 4 times in the Executive Summary (9 times total in the report) to describe specific findings that had no definitive evidence or proof and the word "support" was used two times to describe technical functions that are normal in any ISP environment and have no relevance to actual actions taken by XBT/Webzilla.

53. In contrast, BuzzFeed definitively printed "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"

54. "Using" means active action and/or application that is verifiable. **The FTI report never once uses the word "prove" "proves" or "proof"** and only uses the term "forensic" in reference to forensic accounting in the Qualifications section.

55. The core of this matter revolves around this statement: "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"

56. Assuming, only for the sake of argument, that everything the FTI report was true, there is still no supporting evidence to back up these claims. If proper procedure were followed and a forensic investigation were conducted, the following and most basic of questions, would have been answered and

included in the report for at least the following four categories (virus transmission, plant bugs, steal data, and conduct 'altering operations')

Virus transmission

- What viruses? What virus or malware code was discovered on XBT or XBT affiliate servers, standalone hard drives, USB drives, optical media, etc.?
- What incident response and forensic acquisition procedures were conducted to determine if viruses were present on any XBT systems?
- What logs were reviewed, and by who, proving which virus names and or file signatures that were deliberately launched by an XBT owner or employee?

Plant bugs

The term "plant bugs" typically refers to the covert or illegal installation of a physical listening device in a home or office and is not a term used when referring to digital operations which is regularly referred to as "spyware", something an organization like BuzzFeed would be expected to know or at least verify before publishing an article.

With that novice-level inaccuracy set aside:

- What spyware was discovered on XBT or XBT affiliate servers, standalone hard drives, USB drives, optical media, etc.?
- What incident response and forensic acquisition procedures were conducted to determine if spyware was present on any XBT systems?
- What logs were reviewed, and by who, proving which spyware names and or file signatures that were deliberately launched by an XBT owner or employee?

Steal data

- What data exfiltration malware or other data theft indicators were discovered on Democratic party machines?
- What analysis was done on the data exfiltration malware to determine what data was successfully stolen from Democratic party machines and to where this data was sent?
- Was any of this data found on XBT or XBT affiliate servers, standalone hard drives, USB drives, optical media, etc.?

Conduct 'altering operations'

- What ransomware or destructive malware indicators were discovered on Democratic party machines?
- What analysis was done on this destructive malware to determine what data was successfully ransomed or damaged from the Democratic party machines?
- Was any ransomware or destructive malware or any other "altering operations" code found on XBT or XBT affiliate servers, standalone hard drives, USB drives, optical media, etc.?

57. What is important to emphasize, and highlight is that Mr. Ferrante does not provide a single piece of evidence in response to any of the above questions and/or in support of any of the claims made by the defendants.

9 . Conclusion

58. It is my opinion that the defendants had no factual information or proof to support the claims made against the plaintiffs. I have found that Anthony J. Ferrante's expert report lacks accuracy in the form of misleading technical information and a clear attempt to shift the narrative to put unfair and baseless blame on the plaintiffs. The defendants' report also lacks forensic soundness and the total absence of any established forensic procedures and does not provide any supporting evidence to back the statements made by the defendants.

59. To summarize, below is a copy of the Executive Summary with the words "suggests" and "support" highlighted to illustrate the speculation and baseless conclusions FTI expounded in their report. The last two bullets in the Executive Summary are skewed judgment calls from FTI with no supporting fact and the assumption of guilt by customer association with no supporting evidence. After each claim made by Mr. Ferrante a brief analysis is provided.

> 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.
>
> • 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.
>
> *ANALYSIS – Mr. Ferrante provides no proof that this was the case and the actual IP addresses that were provided by the DNC do not contain the plaintiffs' IP addresses. Therefore, his statement that "technical evidence suggests" is completely false, because he failed to provide any technical evidence.*
>
> • 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.
>
> *ANALYSIS – Mr. Ferrante provides no proof that this was the case and the actual IP addresses that were provided by the DNC do not contain the Plaintiffs' IP*

addresses. Therefore, his statement that "technical evidence suggests" is completely false, because he failed to provide any technical evidence. Even if this statement was true, which it is not, just because something occurred in the past does not mean it is related to current events.

• 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.

ANALYSIS – Once again this is a mischaracterization of how ISPs work and operate and Mr. Ferrante fails to point out that this statement would also apply to many organizations including Amazon and Google.

• 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.

ANALYSIS – Once again this is a mischaracterization of how ISPs work and operate and Mr. Ferrante fails to point out that this statement would also apply to many organizations including Amazon and Google.

• 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.

ANALYSIS – Mr. Ferrante provides no proof that this was the case. It is important to note that Mr. Ferrante is not saying IP addresses were used (which is trued of every ISP), he is saying XBT "support[ed]" the schemes and attacks.

• 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.

ANALYSIS – This statement by Mr. Ferrante is completely false, plus he provides no proof that this was the case. It is important to note that Mr. Ferrante is not saying IP addresses were used (which is trued of every ISP), he is saying XBT "support[ed]" the schemes and attacks. If Mr. Ferrante looked closely at the evidence, he would have realized that most of the IP addresses that were used were not XBT-owned.

• 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.

ANALYSIS – Mr Ferrante provides zero deposition transcripts in his report and shows zero evidence to support this claim. Mr. Ferrante seems to think it is *acceptable to make false claims backed up by zero factual evidence. In addition, whether or not XBT did or did not have adequate enterprise infrastructure is not relevant to the case and would provide no justification for the false and defamatory statements made by the defendants.*

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

ANALYSIS – Mr Ferrante provides zero names of any "credible sources" that name XBT affiliates. If there are public sources and this is credible, why did Mr. Ferrante fail to list the actual names and cite the actual references.

60. In summary, as shown above, Mr. Ferrante's report makes a series of claims with no supporting or factual evidence to back it up. For example, if public records show credible sources, the credible sources should have been listed in his report. This is one of many examples were claims are made with no evidence provide to support the claims.

Dr. Eric Cole

Founder Secure Anchor Consulting, LLC