MALWARE CAPABILITY DEVELOPMENT PATTERNS RESPOND TO DEFENSES: TWO CASE STUDIES

February 2016

Kyle O'Meara
Deana Shick
Jonathan Spring
Edward Stoner

Executive Summary

Adversaries are constantly adding functionality to their tools to evade defense measures deployed by network defenders or software developers. Adversaries adding functionality to their tools avoid almost any simple or known detection technique via a variety of mechanisms. Feature additions make the malware more robust and allow adversaries to use the tool for a variety of use cases beyond the original intent.

This paper uses two case studies to outline the relationship between adversaries and network defenders since feature additions and network defense measures are well known. Zeus is a banking trojan that has been active since 2007 and is used primarily to exfiltrate banking credentials or other financial data from unsuspecting victims. BlackEnergy has been active since early in 2007 and was originally designed to perform distributed denial of service (DDoS) attacks. More recently, BlackEnergy can also degrade the integrity of industrial control systems (ICS).

The progression of the abilities available to actors is a good case study for demonstrating the extent to which cybersecurity is a back-and-forth struggle between adversaries and defenders. The cat-and-mouse nature of the interplay is apparent as Zeus and BlackEnergy continue to add just enough features to stay one step ahead of defensive capabilities. Each minor capability has likely gone through the Adversary Capability Chain (ACC), and by the time they are open source they are evidencing signs of the Ubiquity phase (Spring, Kern, & Summers, 2015).

We point to the resilience of the adversary ecosystem to raise awareness and help defenders anticipate this phenomenon. There is no obvious solution to end the cat-and-mouse game. However, some advice is relevant in light of this state of affairs. When to burn equities is an important decision. That is, when to reveal defensive strategy information to the adversary and permit them to respond, and when to instead hold such information close (Spring & Stoner, 2015).

Introduction

This study adds a new aspect to our current understanding of the malicious code usage and development ecosystem. We previously assessed and demonstrated the futility of using only simple, reactive defenses since adversaries evade simple blacklist detection without a lasting cost to their operations by developing new capabilities (Spring 2013). Spring et al. (2015) models the progression of the community of adversaries to obtain a certain single capability over time. The case studies of Zeus and BlackEnergy feature additions herein are complementary to the model of a single capability's development because the case studies demonstrate the pattern of the community of adversaries gaining a series of such capabilities over time in an organized manner. The capabilities in this series serve different purposes. Some are logistic, serving to maintain control over bots remotely. Some are anti-analysis, preserving adversary control via a different avenue. Yet others are auxiliary.

Each minor capability we note in this study is obscure and thus difficult to track through the whole chain of development. However, the whole set of capabilities and their variety demonstrate the complex nature of the adversary ecosystem. Various minor capabilities such as these are necessary to support the more general adversarial capability of stealing banking information, for example. Defender intervention and new defensive techniques interrupt the total adversary capability to the end goal of theft by interrupting a logistical capability. Despite these continued interruptions, each time the adversary community develops a new capability to restore the overarching capability of banking credential theft.

Case 1: Zeus Feature Addition Timeline

Zeus, a banking trojan, has been in active development since 2007. It is the oldest and most widely deployed trojan. We use Zeus as a case study and exemplar to highlight the cat-and-mouse game between network defenders and adversaries. Zeus was originally sold through Russian-language forums, but became freely available in 2011. Once the code was open source, adversaries repurposed the code repeatedly to avoid detection, exfiltrate data from a variety of sources, and prevent researchers from understanding the tool's capabilities.

Figure 1 highlights features added to Zeus malware over time. The grey diamonds designate features that add new capabilities and the black diamonds represent developments that repurposed Zeus from its original purpose—financial theft.

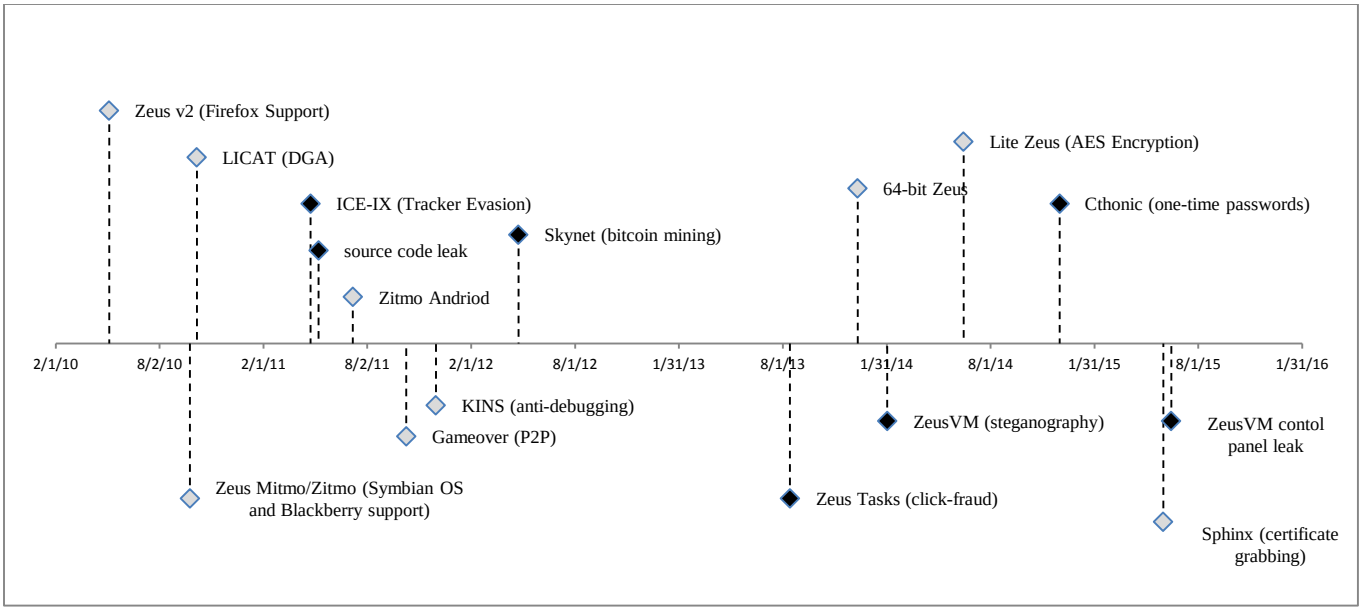

Figure 1: Timeline of Zeus Feature Developments

Figure 1 demonstrates that Zeus receives regular feature updates, very much as it would in many well-run non-malicious software projects. Many features demonstrate the robustness of Zeus because the authors are aware of and have the ability to circumvent countermeasures.

- Zeus, first discovered in 2007, contained keylogger functionality to exfiltrate sensitive information to static command and control (Brewster, 2010).
- Zeus employed fast flux since late 2007 to hide its phishing and malware delivery infrastructure (Stoner, 2010) (Artman, 2007).
- Zeus v2 added support for compromising Firefox, Windows Vista, and Windows 7 in 2010 (Baumhof, 2010). This update enabled the malware to be deployed on many more targets.
- Zeus Mitmo/Zitmo added payloads for Symbian OS and Blackberry in 2010, and later for Android in 2011 (Barroso, 2010), to defeat two-factor authentication used by financial institutions (Apvrille, 2011). The financial institutions deployed two-factor authentication as a countermeasure specifically to the banking trojans.
- Zeus LICAT added domain-generation algorithms (DGA) in 2010 (Manuel, 2010). DGA, pioneered by Conficker malware, provides robust communications by generating numerous pseudo-random names to contact command and control (C2) servers. DGA significantly degrades the effectiveness of defender blacklists (Antonakakis, et al., 2012).
- Gameover Zeus added peer-to-peer (P2P) networking for C2 communications in 2011 as another way to avoid domain-name takedowns. Domain-name takedowns had become an effective countermeasure; however, P2P C2 avoids the DNS entirely, which makes domain-name takedowns useless (Abuse.ch, 2011).
- Zeus KINS added anti-debugging and anti-analysis features in 2011 to prevent cybersecurity researchers from easily deciphering capabilities within the malware (Bijl, 2011).

- Zeus added 64-bit support and TOR support in 2013. 64-bit malware can be deployed on many more target operating systems. Support for TOR, an IP-anonymization network, further evades network analysis and blocking (Tarakanov, 2013).

- ZeusVM added steganographic techniques to retrieve configuration information from seemingly innocuous images in February 2014. Steganography allowed the tool to evade intrusion detection systems (IDS) and anti-virus software (Segura, 2014).

- Lite Zeus was discovered by researchers in June 2014. The malware employed AES encryption to evade detection and prevent researchers from understanding its capabilities (Walker, 2014).

- Cthonic was discovered by researchers in December 2014. Cthonic added functionality for web injections, defeating one-time passwords and pins, and collected camera footage from the victim (Namestnikov, Kuskov, & Kupreev, 2014).

- In August 2015, Sphinx added the ability to grab legitimate certificates to evade security pop-up notices and transparent web-page redirects (Webfakes), and the ability to wage a phishing campaign without redirecting the victim to a malicious domain. All of these functions avoided DNS blocking measures and made networks harder to defend. Additionally, Sphinx routed all traffic through the TOR network to avoid network analysis and blocking measures (Paganini, 2015).

Other features demonstrate how different parties can easily use Zeus and repurpose it.

- The Zeus source code leaked in 2011, and it is still available in github. This availability gives anyone on the Internet access to the code base for free (Kruse, 2011).

- ICE-IX, a Zeus derivative, was identified in 2011. It contains features for evading identification from sinkhole software setup to track Zeus (Abuse.ch, 2011).

- Zeus Skynet appeared in 2012. The author was interviewed on reddit.com and claimed to have added new features to Zeus (such as TOR support and Bitcoin mining), as well as to be operating a ~10k node botnet (Reddit, 2012).

- Zeus Tasks appeared in 2013. It added support for click-fraud. In this particular case, Zeus infected machines in order to generate Instagram followers to computer-generated Instagram accounts, which were then sold (Fielder, 2013).

- ZeusVM (KINS) v2.0.0.0 control-panel source code and builder was leaked and became available to the public in June 2015. This derivative gives anyone on the Internet the ability to build a ZeusVM botnet for free (Constantin, 2015).

- Cthonic repurposed and combined several features found in earlier versions of Zeus in late 2014. Features included AES encryption mechanisms similar to Lite Zeus, virtual machine functionality found in KINS and ZeusVM, and similarities with the Zeus v2 configuration files (Namestnikov, Kuskov, & Kupreev, 2014).

Case 2: BlackEnergy Feature Addition Timeline

BlackEnergy is another example of malware that has been adapted over the years and has gained feature additions to defeat network defenses. BlackEnergy is not open source (i.e., it is not in the Ubiquity phase of capability as Zeus is). The BlackEnergy authors tightly control access to the functionality of the newest versions of the tool. Even though BlackEnergy versions have not become open source, certain versions of the source code were shared and/or sold for a fee (Wolf, 2010).

Although BlackEnergy began life as malware that generated bots to support DDoS attacks, it has evolved into a multi-purpose malware toolkit used to attack an array of sectors. It was originally sold on the Russian underground cyber market; in 2007, it was discovered there by Arbor Networks (Nazario, 2007). Since 2007, researchers have seen four iterations of BlackEnergy.

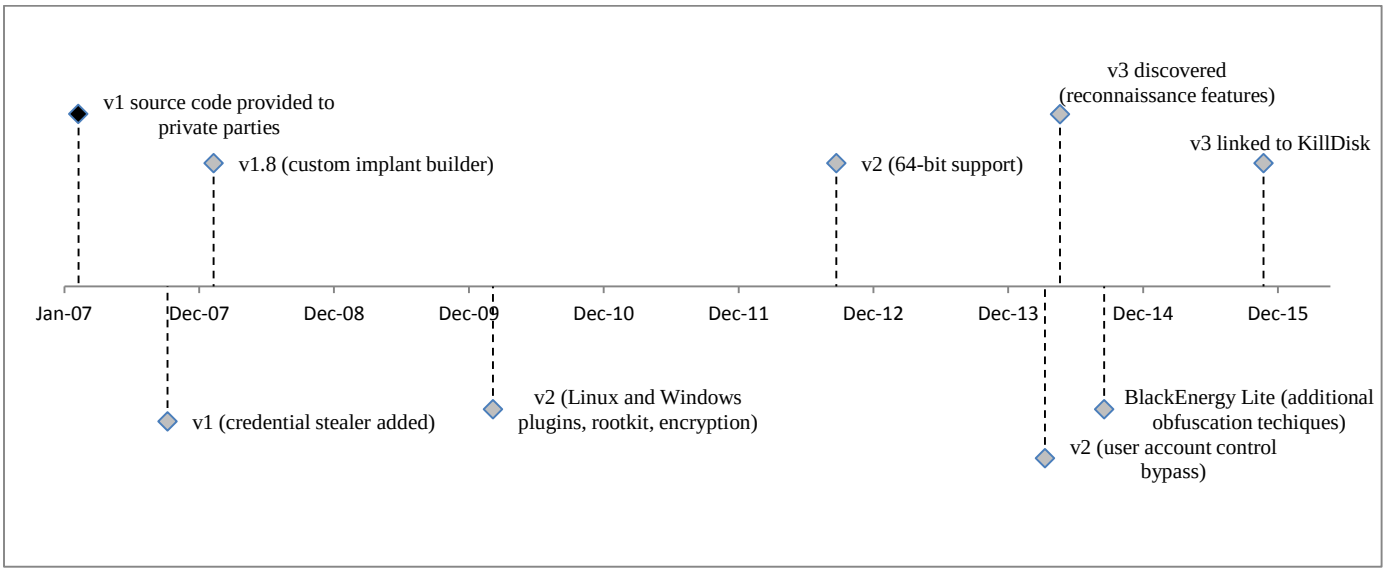

Figure 2: Timeline of BlackEnergy Feature Developments

Figure 2 highlights features added to BlackEnergy malware over time. The grey diamonds designate features that add new capabilities while the black diamonds represent developments that allowed authors to repurpose BlackEnergy from its original purpose. Figure 2 demonstrates that BlackEnergy receives semi-regular feature updates to support targeting a wider breadth of victims, similar in spirit to Zeus but less frequent. Many features demonstrate the robustness of BlackEnergy logistics because its foremost objective as malware is to be able to circumvent defenses.

- BlackEnergy v1 surfaced in 2007. Arbor Networks analysts determined it was a toolkit designed to create botnets for conducting DDoS attacks (Nozario, 2007). It contained server-side scripts that the adversary's command and control (C2) server configured. The C2 servers could distribute the scripts to all bots for easy control and focus attacks on particular victims (F-Secure, 2014).

- BlackEnergy v1.8 included a custom implant builder to evade antivirus protections. It was discovered toward the end of 2007 (Saisyu, 2012).

- BlackEnergy v2 was discovered by researchers in March 2010 (Wolf, 2010) and went through several feature changes from version 1 (Samani, 2016). The tool added functionality via plugins available for Linux and Windows, which included rootkit functions and data encryption. The researchers found much of the code was rewritten from v1, but maintained the original DDoS functionality. The malware used the regedt32.exe installer, which is disguised to look like a typical registry editor tool so that unsuspecting users will execute the program (F-Secure, 2014).

- BlackEnergy v2 added functionality to include support for Windows 64-bit in late 2012, which allowed adversaries to attack a wider scope of targets (F-Secure, 2014).

- BlackEnergy v2 added features in April 2013, which included a user-account control bypass to circumvent security measures that Microsoft had recently added to its Windows operating systems. The malware changed installers to msiexec.exe from regedt32.exe, which evaded detection and tricked unsuspecting users into running the malware (F-Secure, 2014).

- BlackEnergy Lite added new features by removing parts, making it smaller and harder to detect. Researchers discovered this new version in early 2014. Specifically, the new malware had no kernel-mode driver component and fewer plugin functionalities, which was likely designed to obfuscate the malware with a lighter footprint (Lipovski, 2014).

- BlackEnergy v3 emerged in May 2014 using the regedt32.exe installer, but included connections for proxy servers, no driver component, configuration changes, and additional plugins related to reconnaissance and information gathering (F-Secure, 2014).

- In late 2015, researchers linked BlackEnergy v3 to the destructive KillDisk malware, which intentionally damages file systems (Cherepanov, 2016).

BlackEnergy is unlike Zeus in many ways since it is in the Escalation phase of the ACC and not the Ubiquity phase. However, the tool is not exclusive to a single group; several groups appear to have used the tool for various nefarious reasons. Since BlackEnergy v1, adversaries kept new feature additions tightly held and used indefensible methods during operations. Older versions of the tool can be found on malware forums and malware collection organizations such as VirusTotal.

- BlackEnergy v1 source code was released purposefully by the author in 2007, allowing access to a limited number of parties who could use and modify the toolkit. Cyber criminals used the v1 toolkit primarily for financial gain and to disrupt victim networks (Wolf, 2010).

- Organized, nefarious actors attributed to a Russian espionage group used BlackEnergy v3 in October 2014. The operation exploited a zero-day vulnerability in Windows, allowing the attackers remote access into victim networks. The group targeted NATO, the United States, eastern European energy companies, and European governments in the campaign (Ward, 2014).

- The additional plugins found in BlackEnergy v3 allowed the tool to attack nation-state power grids in early 2016. This shift to targeting industrial control systems (ICS) suggested nation-states supported this attack rather than cyber criminals interested in financial gain (Cherepanov, 2016).

Conclusion

Cyber security is a back-and-forth struggle between adversaries and defenders. We elaborated this struggle using two case studies of publicly available information over eight years for the Zeus and BlackEnergy malware families. The nature of this cat-and-mouse relationship is apparent as malware toolkits such as Zeus and BlackEnergy continue to evolve to defeat defensive capabilities.

The lesson from the back-and-forth nature of capability development by these malicious software families indicates it is wise to consider the knowledge of malware capability a kind of computer network defense (CND) equity that will need an appropriate strategy for when to reveal information publicly and when to share it more closely. Although it is tempting to trust that formal mathematics and game theory can provide an easy solution to this problem, based on prior analysis, such formal tools do not provide a complete solution (Spring, 2014). Politics and clever heuristics should be combined with sound evidence and the appropriate mathematical decision support to arrive at a good CND equities strategy.

Bibliography

Abuse.ch. (2011, 4 25). *Ice IX - Or Just ZeuS?* Retrieved 2 11, 2016, from http://www.abuse.ch/?p=3453

Abuse.ch. (2011, 10 10). *Zeus Gets More Sophisticated Using P2P Techniques*. Retrieved 2 11, 2016, from www.abuse.ch/?p=3499

Antonakakis, M., Perdisci, R., Nadji, Y., Vasiloglou, N., Abu-Nimeh, S., Lee, W., & Dagon, D. (2012). From throw-away traffic to bots: detecting the rise of DGA-based malware. *21st USENIX Security Symposium.* Bellevue.

Apvrille, A. (2011, 7 8). *Zitmo hits Android*. (Fortinet) Retrieved 2 11, 2016, from http://blog.fortinet.com/zitmo-hits-android

Artman, J. (2007, 12 11). *Tracking the Russian Business Network (RBN).* Retrieved 2 11, 2016, from RBN Exploit: https://www.cl.cam.ac.uk/research/security/seminars/archive/slides/2007-12-11.pdf

Barroso, D. (2010, 9 25). *Zeus Mitmo: Man-in-the-mobile*. (S21 Security) Retrieved 2 11, 2016, from http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html

Baumhof, A. (2010, 5 6). *Zeus 2.0 - Zeus trojan at its best - extending its reach to Windows Vista, 7 and Mozilla Firefox*. (Tidos Group) Retrieved 2 11, 2016, from http://www.tidos-group.com/blog/2010/05/06/zeus-2-0-zeus-trojan-at-its-best-extending-its-reach-to-windows-vista-7-and-mozilla-firefox

Bijl, J. (2011, 12 1). *Analysis of the KINS malware*. (Fox-IT) Retrieved 2 11, 2013, from http://blog.fox-it.com/2013/07/25/analysis-of-the-kins-malware/

Brewster, T. (2010, 8 10). *Timeline: Three years of Zeus terror*. Retrieved 2 11, 2016, from IT Pro: http://www.itpro.co.uk/625912/timeline-three-years-of-zeus-terror

Cherepanov, A. (2016, January 3). *ESET*. Retrieved January 7, 2016, from We Live Security : http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Constantin, L. (2015, 07). *ZeusVM malware building tool leak may cause botnet surge*. Retrieved from PC World: http://www.pcworld.com/article/2944412/leak-of-zeusvm-malware-building-tool-might-cause-botnet-surge.html

Espiner, T. (2009, 11 19). *UK police make Zeus Trojan arrests*. (ZD Net) Retrieved 2 11, 2016 from http://www.zdnet.com/uk-police-make-zeus-trojan-arrests-3039890509/

Fielder. (2013, 8 14). *New Zbot Variant Builds Instagram Army #INTH3WILD*. (RSA) Retrieved 2 11, 2016, from https://blogs.rsa.com/new-zbot-variant-builds-instagram-army

F-Secure. (2014). *F-Secure Whitepapers.* Retrieved from BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks: https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

Humphries, M. (2010, 9 29). *19 arrested in $9.5 million Zeus trojan bank scam*. Retrieved 2 11, 2016, from http://www.geek.com/news/19-arrested-in-9-5-million-zeus-trojan-bank-scam-1287345/

Kovacs, E. (2016, 1 4). *BlackEnergy Malware Used in Ukraine Power Grid Attacks*. Retrieved from Security Week: http://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks

Kruse, P. (2011, 5 9). *Complete ZeuS sourcecode has been leaked to the masses.* (Center for Strategic and International Studies) Retrieved 2 11, 2016, from http://www.csis.dk/en/csis/blog/3229/

Lipovski, R. (2014, 9 24). *Back in BlackEnergy *: 2014 Targeted Attacks in Ukraine and Poland.* Retrieved 2 11, 2016, from We Live Security - ESET Experts: http://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

Manuel, J. (2010, 10 7). *File Infector Uses Domain Generation Technique Like DOWNAD/Conficker*. (Trend Micro) Retrieved 2 11, 2016, from http://blog.trendmicro.com/trendlabs-security-intelligence/file-infector-uses-domain-generation-technique-like-downadconficker/

Namestnikov, Y., Kuskov, V., & Kupreev, O. (2014, 12 18). *Chthonic: a new modification of ZeuS*. Retrieved from Securelist: https://securelist.com/blog/virus-watch/68176/chthonic-a-new-modification-of-zeus/

Nazario, J. (2007, October 12). *Arbor Networks*. Retrieved February 7, 2016, from BlackEnergy DDoS Bot – Analysis Available: http://www.arbornetworks.com/blog/asert/blackenergy-ddos-bot-analysis-available/

Nozario, J. (2007, 10). *Black Energy DDoS Bot Analysis.* Retrieved 02 11, 2016, from Arbor Networks: http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

Osborne, C. (2013, 4 5). *Suspected hackers behind Carberp botnet Eurograbber arrested*. (ZD Net) Retrieved 2 11, 2016 from http://www.zdnet.com/suspected-hackers-behind-carberp-botnet-eurograbber-arrested-7000013580/

Paganini, P. (2015, 08 26). *Sphinx, a new variant of Zeus available for sale in the underground*. Retrieved from Security Affairs: http://securityaffairs.co/wordpress/39592/cyber-crime/sphinx-variant-zeus-trojan.html

Prince, B. (2010, 10 1). *UK Police Arrest 5 over $70M Zeus Trojan Bank Scheme.* (E-Week) Retrieved 2 1, 2016, from http://www.eweek.com/c/a/Security/FBI-Ukraine-Police-Arrest-5-in-70M-Zeus-Trojan-Bank-Scheme-637534

Reddit. (2012, 4 24). *IAmA a malware coder and botnet operator*. Retrieved 2 11, 2016, from http://www.reddit.com/r/IAmA/comments/sq7cy/iama_a_malware_coder_and_botnet_operator_ama/?limit=500

Saisyu, E. (2012, 2 24). *Black Energy Bot v 1.8 Analysis.* Retrieved 2 11, 2016, from Edisun Industries: http://edisunindustries.blogspot.com/2012/02/black-energy-bot-v-18-analysis.html

Samani, R. (2016, January 14). *McAfee Labs*. Retrieved February 7, 2016, from Updated BlackEnergy Trojan Grows More Powerful: https://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/

Segura, J. (2014, 02 17). *Hiding in plain sight: a story about a sneaky banking Trojan*. Retrieved from MalwareBytes Unpacked: https://blog.malwarebytes.org/security-threat/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/

Shamir, U. (2016, January 26). *Sentinel One.* Retrieved February 7, 2016, from Analyzing a New Variant of BlackEnergy 3 Likely Insider-Based Execution: https://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf

Spring, J. M. (2013). Modeling malicious domain name take-down dynamics: Why eCrime pays. *eCrime Researchers Summit (eCRS)* (pp. 1--9). San Francisco: IEEE.

Spring, J. M. (2014). Toward realistic modeling criteria of games in internet security. *Journal of Cyber Security & Information Systems, 2*(2), 2-11.

Spring, J. M., & Stoner, E. (2015). *CND Equities Strategy.* Pittsburgh, PA: CERT Program, Software Engineering Institute, Carnegie Mellon University.

Spring, J. M., Kern, S., & Summers, A. (2015). Global adversarial capability modeling. *Electronic Crime Research (eCrime)* (pp. 1--21). Barcelona: IEEE.

Stoner, E. (2010). DNS Footprint of Malware. *DNS-OARC.* Denver. Retrieved from https://indico.dns-oarc.net//getFile.py/access?contribId=4&resId=0&materialId=slides&confId=14

Tarakanov, D. (2013, 12 11). *The inevitable move - 64-bit ZeuS has come enhanced with Tor*. (Secure List) Retrieved 2 11, 2016, from https://www.securelist.com/en/blog/208214171/The_inevitable_move_64_bit_ZeuS_has_come_enhanced_with_Tor

United States Department of Justice. (2013, 5 3). *International Cybercriminal Extradited from Thailand to the United States*. (Office of Public Affairs) Retrieved 2 11, 2016, from http://www.justice.gov/opa/pr/2013/May/13-crm-502.html

Walker, D. (2014, 06 30). *SC Magazine*. Retrieved from 'Lite Zeus' has fewer tricks, but updated encryption: http://www.scmagazine.com/lite-zeus-has-fewer-tricks-but-updated-encryption/article/358593/

Ward, S. (2014, 10 14). *iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign*. Retrieved 2 15, 2016, from iSIGHT Partners: http://www.isightpartners.com/2014/10/cve-2014-4114/

Wilson, T. (2010, 9 30). *More Than 80 Arrested in Alleged Zeus Banking Scam*. (Dark Reading) Retrieved 2 11, 2016, from http://www.darkreading.com/attacks-breaches/more-than-80-arrested-in-alleged-zeus-ba/227501125

Wolf, J. (2010, 03 03). *BlackEnergy Crypto.* Retrieved 2 11, 2016, from FireEye Threat Research: https://www.fireeye.com/blog/threat-research/2010/03/black-energy-crypto.html

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0003404