SMALL WARS JOURNAL

OODA LOOPS IN CYBERSPACE: HOW CYBER AWARENESS TRAINING HELPS THREAT ACTORS

http://smallwarsjournal.com/jrnl/art/ooda-loops-cyberspace-how-cyber-awareness-training-helps-threat-actors

Robert Zager and John Zager

Cybersecurity's human adversarial engagement is often lost in discussions of cybersecurity. We discuss how defenders' focus on technology unintentionally creates vulnerabilities which can be exploited by threat actors. In particular, we discuss how the convergence of cyber awareness training and defensive technologies is exploited by threat actors with devastating consequences.

URL Abuse

Attackers want their attacks to look as realistic as possible and they therefore create websites and URLs that look like sites their targeted victims would expect to receive email from or visit.

- Brad Smith, Microsoft President[1]

On August 8, 2018, Microsoft announced that its Digital Crime Unit (DCU) had obtained a United States District Court order transferring control of six internet domains from Strontium, a presumptive affiliate of the Russian government, to Microsoft.[2] The seized domains were associated with foreign efforts to subvert U.S. democracy. The transferred domains were:

- my-iri.org
- hudsonorg-my-sharepoint.com
- senate.group
- adfs-senate.services
- adfs-senate.email
- office365-onedrive.com

Each of these six domains was designed to mimic a legitimate organization that would be of interest to the specific targets. The first domain appeared to be associated with the International Republican Institute, a think tank affiliated with six Republican U.S. Senators. The second was designed to mimic the Hudson Institute, another prominent think tank. The third, fourth and fifth were obviously intended to mimic the U.S. Senate. The last was designed to mimic Microsoft's popular Office 365 service. This is the sixth time in two years that Microsoft has gone to court to seize malicious websites, bring the total seized to eighty-four.

While seizing eighty-four malicious domains is laudable, a review of the six listed domains reveals how easy it is for threat actors to create deceptive domains that must be discovered and then decommissioned. In the six domains, the threat actors used five different Top Level Domains (TLDs), namely, ".org", ".com", ".group", ".services", and ".email'. These are just five of the over 1,500 TLDs that are currently available.[3] The large, and growing, number of TLDs and their respective registrars create a vast universe of possible URLs for threat actors to exploit.

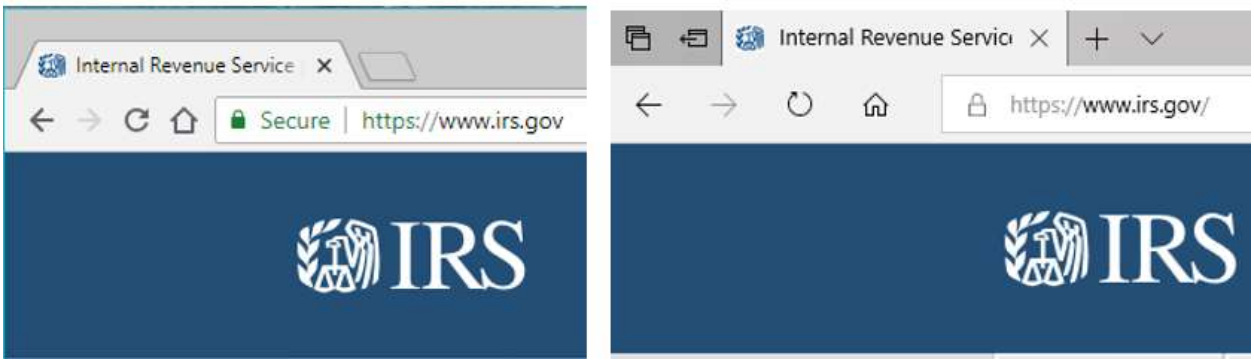
It must be noted that DMARC, the email defensive technology mandated by DHS BOD 18-01, is ineffective against attacks which use these URL abuse techniques.[4] This is because the protections afforded by DMARC only protect the real domain, not domains created and controlled by threat actors. In fact, threat actors can use DMARC to increase the perceived legitimacy of attack domains.

SSL Abuse

Bad Money Drive Outs Good.

- Gresham's Law

Gresham's Law is the economic principle that when two forms of a commodity money with the same face value are in circulation, the more valuable commodity will gradually disappear from circulation, being replaced by the less valuable commodity.[5] We currently see a similar dynamic playing-out in cyberspace. SSL digital certificates are issued by entities called Certificate Authorities (CAs).[6] SSL certificates are used to manage HTTPS, the secure browsing protocol for the World Wide Web. While there are many aspects of HTTPS, the one that is relevant to this discussion is the modification of the user's browser interface based on HTTPS state. In general, when the browser session is secured using HTTPS, the user will receive two visual indicators of HTTPS security. The first indicator is that the text address will display https instead of http. The second indicator is a padlock. Figure 1 illustrates how HTTPS is displayed on the website of the IRS in the Chrome and Edge browsers.[7]



Chrome Edge

Figure 1. IRS Website Illustrating HTTPS.

The Chrome browser informs that user that this is "Secure." What does "Secure" mean in the context of HTTPS? It means that the connection between the user's computer and the website being displayed is encrypted. Encrypting the connection makes it very difficult for third parties

to eavesdrop on the traffic over the connection. This is a vitally important security feature. For example, encryption allows the user to transmit banking credentials and conduct banking business online without fear that banking credentials or financial data will be stolen by eavesdroppers. However, securing the connection to the website from eavesdropping is only part of the system. The system is composed of three elements, i.e., the user, the connection and the website. What does an SSL certificate tell the user about the website? The answer to this question is dependent upon two subtleties of the SSL certificate. The first subtlety is the CA that issued the SSL certificate. The second subtlety is the class of the SSL certificate. The three classes of SSL certificate, in increasing order of veracity, are: i) DV, domain validation; ii) OV, organization validation; and iii) EV, extended validation.

The issuing CA and the class of the SSL certificate are of paramount importance. Just as a silver dime is worth more than a cupro-nickel dime, an EV Certificate issued by DigiCert is worth more than a DV certificate issued by Let's Encrypt. In order to obtain an EV certificate from DigiCert, the website operator must pay an annual fee starting at $234.00[8], provide substantial legal documentation and complete a technically complex installation process.[9] On the other hand, obtaining a DV certificate from Let's Encrypt is free, requires no documentation and does not require manual installation.[10] The intermediate OV certificate, which is not free and requires some documentation[11], receives the same visual indictors as the lowest tier DV certificate in browsing environments. Despite the substantial differences between the CAs and classes of SSL certificates, the vast majority of users are unaware of these differences – the different certificates have the same face value. This means that the HTTPS indicators on websites actually provide users with little guidance in determining if the website at the other end of the secure HTTPS connection is a trusted bank or a threat actor. The unfettered availability of free SSL certificates has, unsurprisingly, proven to be very beneficial to threat actors as they are able to display HTTPS indicators on malicious websites, making high trust websites indistinguishable from malicious ones.[12]

Cyber Security Awareness Abuse

... cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines.

-Dr. Fredrick Chang, Former NSA Director of Research[13]

Colonel John Boyd, USAF (Deceased), developed the Observe/Orient/Decide/Act Loop ("OODA loop") as a military decision-making analytical framework. The OODA loop has since been widely adopted outside of the military.[14] At that heart of this framework is the principle that the target's decisions can be influenced by manipulating the information that the target uses to assess the situation.[15] Boyd observed that the success of this manipulation process is dependent upon anticipating the target's thought processes. In the case of spearphishing, a sophisticated threat actor will anticipate that the target has received cyber security awareness training. Threat actors know that cyber security awareness training always emphasizes the importance of inspecting email addresses and looking for HTTPS indicators. Thus, in creating an attack the threat actor will assume:

1. The targeted individual will inspect the domain name displayed in the email address and may even inspect the URLs in the links. This is why, as Brad Smith observed, the threat actor will adopt a domain name that is deceptively similar to a domain name that the target would expect to see. As was the case in an attack on Russian banks, the deceptive domain name does not need to have any relation to the real domain name. In that case, the threat actors used the domain fincert.net to mimic FinCERT, the Russian bank regulator; FinCERT's actual domain name is cbr.ru.[16] It has always been easy to dream up deceptive domain names and the ever-expanding list of TLD's facilitates threat actors in the creation of deceptive domain names.
2. The targeted individual will look for the HTTPS indicators on the destination website and in links. Thus, the threat actor will use SSL on the malicious website. Free SSLs make it easy for threat actors to use HTTPS indicators on malicious sites.

In the OODA loops of cyberspace, training becomes a vulnerability that is manipulated by threat actors because, knowing what the target is looking for, the threat actor will manipulate this information to deceive the target. This is the problem of psychological manipulation that the ODNI called out in the ODNI's Cyber Threat Framework.[17] **Abusive domain names paired with abusive SSL certificates is a one-two punch that is facilitated, not frustrated, by technology and training.**

Cyber security awareness training is an essential, but insufficient, response to malicious abuse of the user interface. The tables can be turned on the threat actor by providing the user with additional information which satisfies two conditions. First, the additional information must augment existing cyber security awareness training. Second, the additional information must be beyond the reach of threat actors.[18] It is possible to leverage intelligence and existing email technologies to create an email interface which satisfies these conditions, enabling users to quickly and easily unmask attempts to mimic trusted email senders. We discussed such a system in *Improving Cybersecurity Through Human Systems Integration*.[19]

The views expressed herein are the views of the authors and do not reflect the views of Iconix, Inc., or Walmart Inc. or its subsidiaries.

---

1. Smith, Brad. "We Are Taking New Steps against Broadening Threats to Democracy." *Microsoft On the Issues*. Microsoft, 20 Aug. 2018. Web. 20 Aug. 2018. <https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/>.
2. Smith, fn. 1.
3. Anon. "tlds-alpha-by-domain." *Iana.org*. Internet Assigned Numbers Authority, 23 Aug. 2018. Web. 23 Aug. 2018. <http://data.iana.org/TLD/tlds-alpha-by-domain.txt>.
4. Zager, Robert. "DMARC Will Not Make Email Secure." *Infosecurity Magazine*. Reed Exhibitions Ltd, 13 June 2018. Web. 23 Aug. 2018. <https://www.infosecurity-magazine.com/opinions/dmarc-will-not-make-email-secure/>.
5. Anon. "Gresham's Law." *Investopedia*. Investopedia, LLC., n.d. Web. 23 Aug. 2018. <https://www.investopedia.com/terms/g/greshams-law.asp>.

6. Anon. "Certificate Authority." *Wikipedia*. Wikimedia Foundation, Inc., 19 Aug. 2018. Web. 23 Aug. 2018. <https://en.wikipedia.org/wiki/Certificate_authority#Providers>.
7. The display of HTTPS information varies substantially between browsers and devices. See, Olenski, Julie. "How to View SSL Certificate Details in Each Browser and What You Can Learn." *GlobalSign Blog*. GlobalSign, 2 June 2017. Web. 23 Aug. 2018. <https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details/>.The understanding of HTTPS information is further complicated by three classes of SSL certificates. Kemmerer, Chris. "DV OV and EV Certificates." *SSL.com*. Ssl.com, 1 July 2015. Web. 23 Aug. 2018. <https://www.ssl.com/article/dv-ov-and-ev-certificates/>.
8. The requirement to provide money to a registrar creates two problems for threat actors. First, fees impose costs on the threat actor which can impact scaling. In the scope of a state actor's efforts to undermine democratic processes, registration costs are relatively nominal. Second, money creates traceability. Traceability is inconsistent with the objective of plausible deniability.
9. Anon. "Extended Validation SSL Certificates." *Digicert*. DigiCert, Inc., n.d. Web. 23 Aug. 2018. <https://www.digicert.com/ev-ssl-certification/>.
Anon. "How to Install the Extended Validation (EV) Code Signing Certificate." *Digicert Knowledgebase*. DigiCert, Inc., 2 May 2018. Web. 23 Aug. 2018. <https://knowledge.digicert.com/solution/SO20518.html>.
10. Anon. "Let's Encrypt." *Wikipedia*. Wikimedia Foundation, Inc., 19 Aug. 2018. Web. 23 Aug. 2018. <https://en.wikipedia.org/wiki/Let%27s_Encrypt>. The number of Let's Encrypt certificates issued has grown from 1 million on March 8, 2016 to 100 million as of June 28, 2017.
11. Anon. "Organization Validation (OV) TLS/SSL Certificate." *Comodo Certificate Authority*. Comodo CA, n.d. Web. 23 Aug. 2018. <https://www.comodoca.com/en-us/solutions/tls-ssl-certificates/organization-validated-(ov)-ssl/>.
12. Cimpanu, Catalin. "14,766 Let's Encrypt SSL Certificates Issued to PayPal Phishing Sites." *BleepingComputer*. Bleeping Computer LLC, 24 Mar. 2017. Web. 23 Aug. 2018. <https://www.bleepingcomputer.com/news/security/14-766-lets-encrypt-ssl-certificates-issued-to-paypal-phishing-sites/>.
13. Chang, Frederick R., Ph.D., *Guest Editor's column*, The Next Wave, Vol. 19, No. 4, 2012. Web. 20 June 2016. <https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-19-4.pdf>.
14. Anon. "OODA Loop." *Wikipedia*. Wikimedia Foundation, Inc., 2 Aug. 2018. Web. 24 Aug. 2018. <https://en.wikipedia.org/wiki/OODA_loop>.
15. Zager, Robert, and John Zager. "OODA Loops in Cyberspace: A New Cyber-Defense Model." *Small Wars Journal*. Small Wars Foundation, 20 Oct. 2017. Web. 23 Aug. 2018. <https://web.archive.org/web/20171124122437/http://smallwarsjournal.com:80/jrnl/art/ooda-loops-in-cyberspace-a-new-cyber-defense-model>.
16. Ragan, Steve. "Dozens of Russian Banks Phished by Crooks Pretending to Be FinCERT." *CSO*. IDG Communications, Inc., 17 Mar. 2016. Web. 23 Aug. 2018. <https://www.csoonline.com/article/3045437/security/dozens-of-russian-banks-phished-by-crooks-pretending-to-be-fincert.html>.
17. ODNI. "Cyber Threat Framework." *Office of the Director of National Intelligence*. ODNI, n.d. Web. 23 Aug. 2018. <https://www.odni.gov/index.php/cyber-threat-framework>.
18. Conti, Gregory and Edward Sobiesk. "Malicious Interface Design: Exploiting the User," *WWW 2010*, April 26–30, 2010, Raleigh, North Carolina, USA.

19. Zager, John, and Robert Zager. "Improving Cybersecurity Through Human Systems Integration." *Small Wars Journal*. Small Wars Foundation, 22 Aug. 2016. Web. 23 Aug. 2018. <smallwarsjournal.com/index.php/jrnl/art/improving-cybersecurity-through-human-systems-integration>.

Robert Zager

Robert Zager is an inventor and entrepreneur. He has been granted twelve United States patents in the areas of computer networking and email. He holds a BA degree from the University of California, Berkeley and a JD degree from Santa Clara University. He is currently a security researcher at Iconix, Inc. in San Jose, California.

John Zager

John Zager is a psychologist with a penchant for systems analysis. He holds a BA degree in Psychology and an MA degree in Industrial Organizational Psychology from Hofstra University While completing his undergraduate studies he served as an intern for U.S. Senator Kirsten Gillibrand (D, NY). He is currently a People Analytics Manager within Walmart's eCommerce division.