An Assessment of Web Defacements against Government and Military Domains

Thomas J. Holt, Steven M. Chermak
Michigan State University
holtt@msu.edu, chermak@msu.edu

Joshua D. Freilich
John Jay College of Criminal Justice
jfreilich@jjay.cuny.edu

Cyberattacks are pervasive, and pose a severe threat to virtually all government and industry sectors. Many of these attacks are economic in nature, targeting sensitive data or resources. Government and military organizations are also subject to attacks from individuals driven by political, nationalist, or other personal causes. Some actors blame these organizations in some way for harms they (i.e., the actors) have personally or vicariously experienced. These web spaces may also be targeted by cyberattackers who seek to demonstrate their technical expertise to the public.

There is minimal research examining cyberattacks against government and military web spaces, due in large part to the difficulty of accurately measuring these types of attacks. Few official data sources provide a comprehensive enumeration of computer-focused offenses such as hacking.[i] Industry or open-source government resources are rarely available due to underreporting on the part of victims, particularly within private industry over fears of economic loss and a decrease in consumer confidence.[ii] As a result, scholars have used a variety of open source and novel data collection strategies to empirically assess hidden forms of crime, such as hacking and malware.[iii]

Web defacements are one of few highly visible forms of computer hacking due to the publicly accessible nature of websites and attackers' interest in publicizing their skills.[iv] The Zone- H.'[v] website maintains an existing repository of data related to website defacements, and has been active in various forms for more than a decade, providing an outlet for hackers who engage in web defacements to publicly report and/or advertise websites they have defaced.[vi] The repository is similar to the self-claiming strategies that terror and extremist groups employ online to attribute physical attacks to their members.[vii] In fact, tens of thousands of defacements are reported, verified, and noted in this archive, making it a relatively comprehensive data source for research on defacements.[viii]

When a malicious online actor engages in a defacement, they can report their actions to the Zone-H website through an online form where they are asked to provide a hacker handle (i.e., adopted online identity of the individual or group) that is labeled as the "notifier" for the defacement. Respondents are also asked to provide some characteristics about the web defacement. For instance, notifiers often indicate the web domain affected (including the date and time), their nickname, the method used to engage in the defacement through a dropdown menu, and the rationale for the attack. The information is passed along to Zone-H site administrators who validate the claims and, if accurate, archive the defacement so that it can be mirrored in perpetuity on the site.

Zone-H only allows the public to view the last 600 reported and validated defacements through the site, limiting the overall information that may be observed. To assess a wider range of political and social events that may have impacted the potential for defacements, we contacted Zone-H to gain access to all defacements reported to the site between January 1, 2012 and December 31, 2016. Zone=H provided us access to all 2,285,256 total defacements reported to the site during this period, regardless of actor motivation. This analysis focuses on all domains hosted within the U.S., and whose Top Level Domain (TLD) ends in either .gov or .mil. These two domains reflect spaces associated with federal government sites and those operated by various branches of the U.S. military.

Defacements Affecting Government (.Gov) Sites (n=9,712)

There were 9,712 total .gov sites reported during the period of study. Of these defacements, most targeted servers using a Linux operating system variant (81.1%; n=7,539) and defaced the home or main page of the site (62.4%; n=5,744). Many of these attacks were mass defacements 48.4% (n=4,460), where the attacker simultaneously defaced as many pages hosted on a server as possible. Additionally, 43.6% (n=4,012) of these attacks were redefacements, where the attacker targeted the same site repeatedly.

Zone-H allows the reporting attacker to indicate their reason for performing the defacement from a series of seven options: (1) just for fun, (2) as a challenge, (3) to be the best defacer, (4) patriotism, (5) political reasons,(6) revenge against that website, and (7) not available or not reported. Only one response could be provided at a time, making each incident associated with a specific motive.

Most attackers targeting .gov sites were driven by a desire to have fun (36.4%; n=3,355), though the next largest category was not identified (24.1%; n=2,216). Some reported attacking sites out of a desire to be the best defacer (16.5%; n=1,522). Political reasons (8.8%; n=811), revenge (6%; n=555) and patriotic reasons (3.9%;

n=360) were also reported in small numbers. A small proportion also reported doing it for the sheer challenge associated with the hack (4.3%; n=393).

Respondents could also report the way in which the attack was completed. Reporters indicated that a majority of defacements used server intrusion methods (21.1%; n=1,942), SQL injection (16.3%; n=1,503), and file inclusions (7%; n=642). A small proportion reported the use of undisclosed or new vulnerabilities (2.8%; n=260), though the use of known vulnerabilities against unpatched systems were far more common (8.7%; n=801). A small number of attacks also involved attacking misconfigured systems (1.4%; n=130), brute force attacks against system resources (2.4%; 227), and social engineering campaigns (1.1%; n=102). Attacks involving these methods (13.6% total) could have been prevented through various security strategies. As a result, there is a clear need for better messaging to ensure situational awareness among system administrators and staff to avoid exposures to social engineering campaigns, and careful implementation of security patching, software updates, and password management to limit potential ingress.

Defacements Targeting Military (.mil) Sites (n=949)

There were 949 total defacements affecting military web sites in this sample, with many attacks affecting the homepage of sites (48.4%; n=459). Most of these attacks were mass defacements (59.6%; n=566), though only a small proportion were redefacements (16.4%; n=156). The majority of these defacements also attacks targeted Linux systems (84%; n=797).

Examining the motivations of defacers revealed most targeted sites for fun or entertainment (50.9%; n=483), followed by no reported reason (17.8%; 169). A proportion also defaced sites because they want to be the best defacer possible (11.4%; n=108). A small proportion of all attacks were performed for more ideological reasons, including political (6.3%; n=60), revenge (5.9%: n= 56), and patriotic reasons (2.7%; n=26).

A range of attack methods were reported by respondents, with some differences compared to government websites. First, the majority of attacks were performed through the use of known vulnerabilities (17.3%; n=164), followed by SQL injection (15.4%; n=146) and no given attack method (13.9%; n=132). Inclusion based attacks were also common (22.6%; 214). Undisclosed vulnerabilities were also relatively uncommon (2.5%: n=24). Social engineering was also less common (1.8%: n=17), as were brute force attacks (2.7%; n=26), and misconfigurations and errors on the part of the administrators (4.5%: n=43).

Discussion

Our analysis demonstrates that many attackers who deface critical government and military websites do so repeatedly. Most of these attacks were not committed to further an ideological cause, but rather because the attacker sought to entertain themselves or demonstrate their skill. Since these sites are attractive targets to cyber-attackers, it is vital that to make them as secure as possible from simple attacks.

To that end, many of these attacks could have been at least partially reduced by improving these websites' cybersecurity posture. There is a clear need for better messaging to ensure that system administrators and staff have situational awareness to avoid exposures to social engineering campaigns. In addition, system administrators and staff must be trained to carefully implement security patching, software updates, and use password management to limit potential ingress. Such measures would reduce the likelihood of success from low-skill attackers driven by various motives.

---

[i] Holt and Bossler, *Cybercrime in Progress*; Holt, Burruss, and Bossler, "Assessing the Macro-Level,"; Wall, *Cybercrime.*

[ii] Brenner, *Cyberthreats;* Holt and Bossler, *Cybercrime in Progress;* Holt, Stonhouse, Freilich, and Chermak, "Examining Ideologically Motivated Cyberattacks,"; Wall, *Cybercrime.*

[iii] Dupont, Cote, Boutin, and Fernandez, "Darkode,"; Holt, Burruss, and Bossler, "Assessing the Macro-Level,"; Leukfeldt, Kleemans, and Stol, "Origin, Growth, and Criminal Capabilities,"; Maimon, Kamerdze, Cukier, and Sobesto, "Daily Trends and Origin."

[iv] Jordan and Taylor, *Hacktivism and Cyberwars;* Woo, Kim, and Dominick, "Hackers."

[v] Zone H, "News."

[vi] Woo, Kim, and Dominick, "Hackers."

[vii] Jennifer V. Carson, Gary LaFree, and Laura Dugan, "Terrorist and non-Terrorist Criminal Attacks by Radical Environmental and Animal Rights Groups in the United States, 1970-2007," *Terrorism and Political Violence* 24, no. 2 (2012): 295-319; Freilich, Chermak, Belli, Gruenewald, and Parkin, "Introducing the United States."

[viii] Woo, Kim, and Dominick, "Hackers."