13

Cyber Hygiene Can Support Cyber Peace

Megan Stifel, Kayle Giroud, and Ryan Walsh[*]

Among high-profile cybersecurity incidents over the past decade, several were reportedly the work of nation-state actors. The actors leveraged tactics, techniques, and procedures to take advantage of known vulnerabilities – technical and human – to undertake actions that compromised personal information, risked human health, and paralyzed the global supply chain. Left unchecked, the scale and breadth of such actions can threaten international stability. Yet, an examination of high-level cases suggests that basic cyber hygiene is an accessible and practical approach to mitigate such incidents, enhance confidence in the use of information and communications technology (ICTs) and, ultimately, advance cyber peace.

[*] About the Global Cyber Alliance.

Founded in 2015 by the District Attorney for New York, the City of London Police, and the Center for Internet Security, the Global Cyber Alliance (GCA) is a charitable organization dedicated to reducing cyber risks. The GCA accomplishes this mission by uniting global communities, scaling cybersecurity solutions, and measuring their impact. In the five years since its launch, GCA has grown to include over 150 organizations as partners, across over thirty countries, and all sectors of the economy. Partner organizations include industry, governments, academia, and other nonprofit organizations.

Examples of GCA's work include support for Domain-based Message Authentication, Reporting, and Conformance – email security protocols known as DMARC, the development of a protective domain name service (DNS), and the creation of cybersecurity toolkits for at-risk organizations and populations. In supporting DMARC, GCA developed a leader board of domains that have fully implemented the tool, conducted multiple boot camps to train administrators on the proper implementation of DMARC, and translated resources guides into eighteen languages. A 2018 study (Shostack et al., 2018) found that the estimated value to the 1,046 organizations that deployed DMARC at a policy level of "reject" or "quarantine," after using GCA's tool, is likely $19 million (USD).

GCA developed a protective DNS service called Quad9 in collaboration with IBM and Packet Clearing House. Quad9 protects users from accessing known malicious websites by leveraging threat intelligence from multiple industry leaders and blocks an average of over 15 million threats per day for users in over eighty-eight countries. A 2019 study (Shostack et al., 2019) found that the use of DNS firewalls can prevent more than 33 percent of cybersecurity data breaches from occurring.

More recently, GCA combined these projects with free resources from software application developers to develop cybersecurity toolkits for small business, elections administrators, and journalists. The toolkits recommend resources to help these organizations and individuals implement internationally recognized cybersecurity best practices. Each toolkit includes several tools, together with

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press

Ninety-one percent of cybersecurity incidents begin with a phishing email (FireEye, 2018). In a phishing attack, a malicious actor poses as someone else and sends an email to a victim in order to trick the victim into taking a particular action – often clicking a link that can give the malicious actor account credentials or access to the victim's device. In the absence of multifactor authentication, accounts and devices compromised via phishing or other means can be leveraged for further exploitation. Actors attributed to nation-states have successfully deployed these tactics in a number of high-profile incidents, including the phishing attacks against staff of the Office of Personnel Management (OPM) in 2015, the Democratic National Committee in 2016, and various organizations in 2020.

1 OFFICE OF PERSONNEL MANAGEMENT

In 2015, the global community learned that actors attributed to China were allegedly accessing the email accounts of top US government officials. Also in 2015, information technology staff at the Office of Personnel Management (OPM) discovered that personnel files had been compromised (Fruhlinger, 2020). Among the personnel files that were accessed were approximately 4 million SF-86 forms, which contain extremely personal information, as well as fingerprint records, gathered in background checks for people seeking US government security clearance (Fruhlinger, 2020). After initially obtaining copies of manuals and other network architecture documents the actors moved laterally throughout the network, which had not implemented multifactor authentication. Public reports suggest the actors explored the network for three years before they were discovered and that the incident affected more than 21.5 million individuals (Starks, 2016).

Further exacerbating the initial breach, after the OPM discovered the compromise, it offered employees a credit and identity protection plan. Almost immediately after OPM sent email notifications to register for their credit monitoring services phishing messages appeared (Vaughan-Nichols, 2015). Malicious actors with knowledge of the planned offering leveraged it to obtain account credentials and personal information from OPM staff. While some staff did login and gave the actors access to their personal information, others stopped before entering their data. Cybersecurity awareness training is said to have, in part, limited the impact of the credit monitoring phishing campaign (Rein, 2015).

brief overviews of the need for the tool and step-by-step instructions to guide users through the tools' set up. A community forum and learning management system further support users in their use of the resources. The toolkit for small business is available in four languages, and GCA is assessing methods to measure the toolkits' impact.

GCA works to eradicate cyber risk and improve the connected world. GCA projects focus on the most prevalent cyber risks individuals and businesses face by developing and deploying practical solutions that measurably improve the security of the digital ecosystem; GCA offers these resources at no cost to the global community. GCA is dedicated to increasing cyber awareness and hygiene across all layers of society through awareness-raising campaigns and civil society engagement.

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press

2 DEMOCRATIC NATIONAL COMMITTEE

On March 19, 2016, John Podesta, the then chair of Hillary Clinton's presidential campaign, received an email purporting to be a Google security alert. Podesta clicked on the link and entered his password into a fake Google log on page through which the actors collected his username and password. As a result, the actors gained access to a decade of his emails (Lipton, 2016). Months later, on October 9, WikiLeaks began publishing thousands of Podesta's compromised emails. Subsequently, several cybersecurity firms attributed the attack to a Russian intelligence unit code-named "Fancy Bear," which has been active since the mid-2000s, and is known among other things for its technique of registering domains that closely resemble domains of legitimate organizations they plan to target. Fancy Bear has also been linked publicly to intrusions into the German Bundestag in 2015, among other intrusions.

3 "MUSTANG PANDA"

January 2020 witnessed a surge in registered domains related to the coronavirus, followed by a spike of cyber incidents. According to Recorded Future's report (Gorey, 2020), malicious actors use COVID-19 as phishing lures for malware, and at least three cases have potential links to nation-state actors. Among them, the "Mustang Panda" campaign has alleged ties to a Chinese government-linked group. The lure used in this campaign was a file discussing COVID-19, purporting to be from the Vietnamese prime minister, Nguyen Xuan Phuc. Once opened, a malicious code could take over the system. Additionally, countries such as the United States, Italy, Ukraine, and Iran have been the focus of related phishing attempts. Malicious actors used trusted organizations as lures for their scam emails, such as pretending to be the World Health Organization and US Centers for Disease Control and Prevention. The malicious emails often use language creating a sense of urgency, or attachments, or links that are said to contain additional information.

At least three cyber hygiene resources can prevent or reduce attacks like the three just mentioned. These resources include deploying Domain-based Message Authentication, Reporting, and Conformance (DMARC), using a protective Domain Name System (DNS), and enabling multifactor authentication. None of these resources alone can prevent a significant cyber incident 100 percent of the time, and they do require investment in human capital. Nonetheless, when implemented across the ecosystem they can have a significant impact. At a minimum, their use can force malicious actors to change targets, tactics, techniques, and procedures. By limiting the impact of phishing and the incidents that may follow, the ecosystem can stabilize, which can support cyber peace.

DMARC is an email authentication, policy, and reporting protocol. DMARC builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From.") domain name, published policies from recipient handling of

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press

authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email. DMARC allows the sender to indicate that their messages are protected and tells the receiver what to do if one of the authentication methods passes or fails – either send the message on or reject the message to junk. DMARC also prevents the dissemination of fraudulent email from an organization's domain. DMARC deployment is a public sector requirement in Australia, Canada, Denmark, the Netherlands, the United Kingdom, and the United States. Moreover, beyond good policy, DMARC prevents significant losses to the global economy. A 2018 study found that the estimated value to the 1,046 surveyed organizations that deployed DMARC at a policy level of "reject" or "quarantine" approached $19 million (USD) (Shostack, Jacobs, & Baker, 2018).

The use of multifactor authentication (MFA) provides an additional effective, low-cost barrier to phishing attacks. A recent survey found that 74 percent of breaches were the result of abuse of privileged credentials (Columbus, 2019). Phishing attacks are one technique used to obtain passwords for use in future exploitation. MFA involves the use of a password plus an additional source of validation, such as a one-time token, to verify a user before granting access to an account. Where enabled, MFA can prevent a malicious actor from using a compromised password to access an account or, in the case of OPM, moving practically uninhibited throughout a vast organizational network.

Additionally, configuring a protective DNS on home and organizational routers can help protect Internet-connected devices against malicious activity. A protective DNS prevents access to known malicious domains by not resolving the DNS query. In doing so, the protective DNS prevents access to a range of threats including malware, ransomware, phishing attacks, viruses, malicious sites, and spyware. Furthermore, using a protective DNS can provide organizations with metrics about the health of their networks and can inform organizational, including national level, incident response functions in the event of a successful attack. One such service, Quad9, protects users from accessing known malicious websites by leveraging threat intelligence from multiple industry sources and blocks an average of over 15 million threats per day for users in over 88 countries. A 2019 study found that the use of DNS firewalls can prevent more than 33 percent of cybersecurity data breaches from occurring (Shostack, Jacobs, & Baker, 2019). The UK Cabinet Office has mandated the use of protective DNS by the public sector. The US Cybersecurity and Infrastructure Security Agency (Nyczepir, 2020) and the National Security Agency are also piloting similar services for their communities of interest (Baksh, 2020).

More recently, actors attributed to nation-states have also capitalized on organizations' failure to patch software and backup data to cause unprecedented losses to the global economy. The Wanna Cry and NotPetya cyberattacks are examples of these incidents. In light of these tactics, two additional best practices can further limit the ability of malicious actors, acting on their own behalf or on behalf of nation-states, from using ICTs to destabilize international order.

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press

4 WANNACRY

In 2017, actors reportedly affiliated with the government of North Korea used ransomware to cripple computer systems around the world (Latto, 2020). The attack was an example of crypto-ransomware, a type of malicious software used by cybercriminals and other actors to extort money. Ransomware accomplishes this by either encrypting valuable files, rendering them unreadable, or by locking the computer, rendering the computer unusable. Like other types of crypto-ransomware, this attack, dubbed WannaCry, took data hostage, promising to return it upon payment of the ransom.

WannaCry began in May 2017 and spread through computers operating Microsoft Windows (Latto, 2020). Users' files were held hostage, and the actors demanded a Bitcoin ransom for their return. The cybercriminals responsible for the attack took advantage of a previously disclosed vulnerability for which a patch was available. Unfortunately, many individuals and organizations had not regularly updated their operating systems and so were left exposed to the attack. The WannaCry ransomware attack impacted approximately 230,000 computers across 150 countries in just one day – many of them belonging to government agencies and hospitals, including thousands of National Health Service (NHS) hospitals and surgery centers across the United Kingdom (Latto, 2020). The attack affected a third of NHS hospitals, with estimated costs of £92 million after 19,000 appointments were canceled as a result of the attack (Field, 2018). Globally, losses due to WannaCry have topped $8 billion USD (Lemos, 2020).

5 NOTPETYA

The 2017 NotPetya attack offers another example of the importance of maintaining up-to-date software. In NotPetya, actors attributed to Russia launched destructive malware adapted from a series of vulnerabilities common to unpatched Windows operating systems. More specifically, they combined the exploit used in WannaCry together with a password harvesting tool called MimiKatz (Greenberg, 2018). By exploiting vulnerabilities in applications in wide use by the private and public sectors, the NotPetya attack quickly spread from targeted Ukrainian banks, payment systems, and federal agencies to power plants, hospitals, and other systems worldwide. Global companies, including Maersk, Merck, and Mondelez, found their systems impacted, with total losses approaching $10 billion USD (Greenberg, 2018). To date, NotPetya is the costliest attack to ever occur. Yet, had the computers been patched, NotPetya likely would have had far less of an impact because it would have had fewer unpatched systems to leverage into patched systems.

Most recently, in September 2020, a woman in Germany reportedly died after the hospital proximate to her was the victim of a ransomware attack, leading to delay in her care. This incident is the first death publicly attributed to a ransomware attack.

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press

Unfortunately, a 2020 study found that 80 percent of observed ransomware attacks in the first half of 2020 used vulnerabilities reported and registered in 2017 and earlier – and more than 20 percent of the attacks used vulnerabilities that were at least seven years old (CheckPoint, 2020). Thus, without a significant shift by key stakeholders within the ecosystem, particularly governments and entities that develop and maintain connected systems, it will likely not be the last.

These ransomware incidents highlight the importance of enabling automatic software updates where appropriate for the operating environment, and otherwise establishing policies for the prioritization and installation of updates. In addition to ensuring software is up to date, appropriately maintained file backups can also mitigate the risk of ransomware. Ransomware targets that maintain clean and timely backups are often able to avoid significant impact from an attack and continue operations without major delays.

6 CONCLUSION

These cases illustrate that the threat from the malicious use of ICTs is real and that known, effective, accessible, and low-cost resources exist to prevent and limit this threat. Still, reducing cybersecurity risk is a continuous process that requires the use of multiple tools together with human capital. Unfortunately failure to employ cyber hygiene collectively has contributed to significant losses globally, including human life. With the increasing, unavoidable dependence on ICTs for everything from governance and economic development to social engagement, inaction becomes increasingly perilous, especially for governments.

Promisingly, an increasing number of national policies are beginning to require the use of cyber hygiene measures in the public sector. This trend reflects a future reality where use of these capabilities is no longer an option, it is the norm. As a result, a state failing to support their implementation may eventually become the cyber equivalent of a safe harbor. Ultimately, despite what society is often led to believe, what stands in the path of cyber peace is not technology, but political will.

REFERENCES

Baksh, M. (2020). NSA piloting secure domain name system service for defense contractors. *Nextgov*. Retrieved October 28, 2020, from www.nextgov.com/cybersecurity/2020/06/nsa-piloting-secure-domain-name-system-service-defense-contractors/166248/

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of global politics*. Harvard University Press.

Center for Internet Security. (Unknown). Ransomware: Facts, threats, and countermeasures. Retrieved October 2, 2020, from www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/

CheckPoint. (2020). Cyber attack trends, mid-year report. *CheckPoint*. Retrieved October 29, 2020, from www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2020.pdf

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press

Columbus, L. (2019). 74% of data breaches start with privileged credential abuse. *Forbes*. Retrieved April 21, 2020, from www.forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/#7bd92a33ce45

Field, M. (2018). WannaCry cyber attack cost the NHS 92m as 19,000 appointments cancelled. *The Telegraph*. Retrieved September 22, 2020, from www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

FireEye. (2018). Email Threat Report. Retrieved October 30, 2020, from www.fireeye.com/offers/rpt-email-threat-report.html

Fruhlinger, J. (2020). The OPM hack explained: Bad security practices meet China's Captain America. *CSO*. Retrieved April 21, 2020, from www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gorey, C. (2020). National-state actors may be running phishing scams that exploit the coronavirus. Siliconrepublic. Retrieved May 5, 2020, from www.siliconrepublic.com/enterprise/coronavirus-phishing-scams

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. Retrieved September 22, 2020, from www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.

Latto, N. (2020). What Is WannaCry? *Avast Academy*. Retrieved April 22, 2020, from www.avast.com/c-wannacry

Lemos, R. (2020). Three years after WannaCry, ransomware accelerating while patching still problematic. *DarkReading*. Retrieved October 29, 2020, from www.darkreading.com/attacks-breaches/three-years-after-wannacry-ransomware-accelerating-while-patching-still-problematic/d/d-id/1337794

Lipton, E., Sanger, D., & Shane, S. (2016). The perfect weapon: How Russian cyberpower invaded the U.S. *The New York Times*. Retrieved April 21, 2020, from www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Nyczepir, D. (2020). CISA looks to offer a new DNS resolver to civilian agencies and beyond. *FedScoop*. Retrieved October 28, 2020, from www.fedscoop.com/cisa-dns-resolver-recursive/

Rein, L. (2015). Reacting to Chinese hack, the government may not have followed its own cybersecurity rules. *Washington Post*. Retrieved October 30, 2020, from www.washingtonpost.com/news/federal-eye/wp/2015/06/18/reacting-to-chinese-hack-the-government-may-not-have-followed-its-own-cybersecurity-rules/

Shostack, A., Jacobs, J., & Baker, W. (2018). Measuring the impact of DMARC's part in preventing business email compromise. Global Cyber Alliance. Retrieved September 22, 2020, from www.globalcyberalliance.org/wp-content/uploads/GCA-DMARC-Exec-Summary.pdf

Shostack, A., Jacobs, J., & Baker, W. (2019). The economic value of DNS security. Global Cyber Alliance. Retrieved September 22, 2020, from www.globalcyberalliance.org/wp-content/uploads/GCA-DNS-Exec-Summary-Report.pdf

Starks, T. (2016). House report: Massive OPM breaches a 'failure' of leadership. *Politico*. Retrieved October 29, 2020, from www.politico.com/story/2016/09/opm-cyber-hacks-house-report-227817

Vaughan-Nichols, S. (2015). Phishing e-mail delays OPM hack remediation efforts. *ZDNet*. Retrieved April 22, 2020, from www.zdnet.com/article/phishing-e-mail-temporarily-stops-opm-hack-remediation-efforts/

https://doi.org/10.1017/9781108954341.013 Published online by Cambridge University Press