GLASSWALL

Elections:

Security is the Easy Part – Society Must Address More Difficult Challenges

glasswallsolutions.com

GLASSWALL

"Probability…carries so much convincingness with it that it naturally determines the judgment and leaves us with no freedom whether to believe or disbelieve, just as a demonstration leaves us with no freedom whether to know or remain ignorant. Things become harder when testimonies contradict common experience, and the reports of history and witnesses clash with the ordinary course of nature or with one another. When that happens we need to use diligence, attention, and exactness if we are to form a right judgment, and to proportion our assent to the credibility and probability of the thing."[1]

I. Introduction

Executive Summary

Since the 2016 U.S. presidential election, much has been published regarding influence operations, Russian hacking and the security of election infrastructure. The biggest lesson learned from 2016 is that the issue of "election security" is vastly more complex and challenging than the narrow focus on election officials securing voting machines and supporting election infrastructure.

While risk stemming from potential exploits of election infrastructure and the systems and data maintained by political parties and candidates must be treated appropriately, it is only a component of election risk requiring attention. A holistic effort to manage risk connected to foreign interference is necessary to ensure that democratic institutions, such as elections, are preserved.

[1] John Locke, An Essay Concerning Human Understanding in Four Books, (London, 1689), Bk. IV, Ch. XVI, p. 265. Available at: <https://www.earlymoderntexts.com/assets/pdfs/locke1690book4.pdf>.

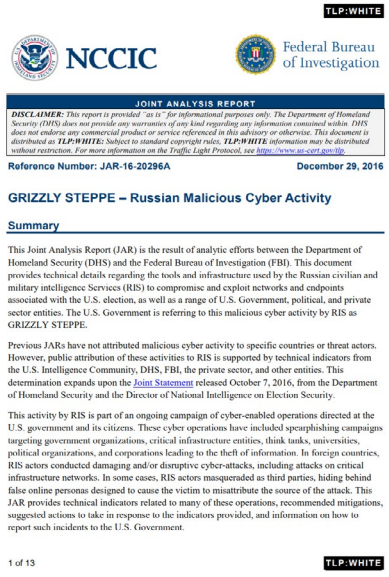
The Threat is Real

On December 29, 2016, the U.S. Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) released Joint Analysis Report (JAR) 16-20296A. Titled "Grizzly Steppe – Russian Malicious Cyber Activity," the report provided "technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities."[2] This JAR and a subsequent NCCIC enhanced analysis provide a detailed view of tactics, techniques and procedures used by two Russian threat actor groups to conduct operations, including "spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information."[3]

The report describes Russian activities that began in mid-2015. It is clear, however, that such foreign interference in democratic institutions did not end with the report's publication or the U.S. government's attribution of such interference to Russia. On August 2, 2018, the U.S. Director of National Intelligence, Dan Coates, disclosed that:

In regards to Russian involvement in the midterm elections, we continue to see a pervasive messaging campaign by Russia to try to weaken and divide the United States. These efforts are not exclusive to this election or future elections, but certainly cover issues relevant to the election.

We also know the Russians tried to hack into and steal information from candidates and government officials alike. We are aware that Russia is not the only country that has an interest in trying to influence our domestic political environment. We know there are others who have the capability and may be considering influence activities.[4]



TLP:WHITE

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296A **December 29, 2016**

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

1 of 13 TLP:WHITE

---

[2] DHS NCCIC and FBI, "GRIZZLY STEPPE – Russian Malicious Cyber Activity", JAR-16-20296A (December 29, 2016), p. 1. Available at: < https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf>.

[3] Id.

[4] Director of National Intelligence, The White House, "Press Briefing by Press Secretary Sarah Sanders and National Security Officials" (August 2, 2018). Available at: <https://www.whitehouse.gov/briefings-statements/press-briefing-press-secretary-sarah-sanders-national-security-officials-08022018/>.

Private sector information technology companies, such as Facebook, Twitter, Microsoft and FireEye, also have disclosed the detection and mitigation of infrastructure established to support foreign influence operations. And a recent article described multiple distributed denial of service attacks on the website of a candidate for congressional office in California. Election infrastructure and the networks and data belonging to candidates for office are at risk.

Also targeted are the public perceptions of political, social and economic issues considered daily by the citizens of Western democracies. As indicated by the U.S. Secretary of Homeland Security, Kirstjen Nielsen, "[o]ur democracy itself is in the crosshairs. Free and fair elections are the cornerstone of our democracy, and it has become clear that they are the target of our adversaries, who seek…to sow discord and undermine our way of life."[5] These are separate but related challenges requiring action.

II. The Long View Challenge

While the threat to election infrastructure, such as voting systems and voter registration databases, is real and carries potential risk, perhaps a more insidious threat targeting this democratic institution is from foreign influence operations. The Federal Bureau of Investigation includes within this category of operations, "covert actions by foreign governments to influence U.S. political sentiment or public discourse," noting that the operations' goals are "to spread disinformation, sow discord, and, ultimately, undermine confidence in our democratic institutions and values."[6] The obvious cases in point are the several reported concerted Russian efforts to "hack" domestic perceptions and public opinion around elections and other matters put to a public vote in the United States and other Western countries. In the months following the U.S. 2016 election, the extent to which threat actors harvested information through spear phishing and other attack vectors to gain access to sensitive data received great public attention. Subsequently, the extent to which foreign actors used and manipulated social media became much more apparent. While government and the private sector can work with political parties, candidates and their respective staff to increase the security around their sensitive information, the broader influence operations using social media present a greater challenge, and one to be tracked and managed over the coming years.

With respect to the latter challenge, there is a need in the United States and other democratic countries to balance countermeasures with the freedoms of speech, assembly and the press.

---

5 Secretary of Homeland Security, White House Press Briefing (August 2, 2018).

6 Federal Bureau of Investigation, "The FBI Launches a Combating Foreign Influence Webpage" (August 30, 2018), available at: < https://www.fbi.gov/news/pressrel/press-releases/the-fbi-launches-a-combating-foreign-influence-webpage>.

This is where U.S. federal, state and local governments are and will remain cautious in taking action on social media content as this can bring them into close proximity with constitutionally-protected freedoms. Even social media platform providers have expressed discomfort with addressing content on their platforms. However, terms of service have given them room to act. Over the last few months, Facebook, Twitter and Microsoft have publicly identified and messaged their remediation of suspected Russian and Iranian websites and taken down thousands of phony social media accounts.[7] There are at least three broad avenues of opportunity for the government, the private sector, academia and non-profit communities to collaborate in this space. Whereas cybersecurity solutions designed to protect infrastructure can be implemented in fairly short-order, subject to the availability of resources and the presence of sufficient will and enterprise governance structures, countering foreign influence operations requires that Western democracies commit to a "long view" for success—outcomes that may take years to realize real results.

In the short-term, government and private sector resources will likely detect the presence of fake websites and social media accounts. This information can be shared and technology companies can investigate, assess whether their terms of service have been violated and then take appropriate actions.

Second, when disinformation campaigns are identified, the targets of those campaigns can counter with objective, factual information that refutes a foreign actor's propaganda.

The third, and perhaps most challenging—but also most important—effort is one where government needs to play a minimal, though supporting, role. This effort will take time to achieve results. Democratic societies need to come to terms with their susceptibility to foreign influence operations in the context of radical changes within the news media and technology sectors over the last few decades. Just as in-depth print media gave way to an often more concise, but perhaps less rich, radio and then television news reporting structure, eventually with a 24-hour news cycle, traditional broadcast media now shares the electro-magnetic spectrum with online news sources, including 280-character "stories". This is not to denigrate the evolution of the information sharing space. For instance, these advances have enabled news reporting from a much broader "sensor" array. Stories that might not have previously been reported can now find their way into mainstream awareness.

//

Democratic societies need to come to terms with their susceptibility to foreign influence operations

[7] See, e.g., Laura Hautala, "How Microsoft spotted another Russian Hacking Attempt" (August 21, 2018), available at: < https://www.cnet.com/news/how-microsoft-spotted-another-russian-hacking-attempt/>; and see, Reuters, "Facebook, Google and Twitter remove hundreds of accounts from Russia and Iran that tried to influence US elections" (August 22, 2018), available at: < https://www.cnbc.com/2018/08/22/facebook-and-twitter-dismantle-disinformation-campaigns-tied-to-iran-and-russia.html>.

In many ways, these changes have supported a march towards increased democratization of news reporting, not far from the purpose Alexis de Tocqueville assigned to a free press where:

Equality sets men apart and weakens them; but the press places a powerful weapon within every man's reach, which the weakest and loneliest of them all may use.[8]

However, society has not fully evolved alongside these changes. It has yet to internalize and control for the vast number of sources contributing to each social media platform, nor for the velocity at which those contributions traverse the Internet and find themselves consumed by individuals. However, traditional guards against falsities, such as publication procedures and fact-checking, are not in place. "News reports of actual events [can be] presented alongside false ones, making it hard for readers to differentiate between them."[9]

In the 1970s, a U.S. Air Force colonel, John Boyd, developed his concept known as the "OODA Loop", with "OODA" standing for "Observe-Orient-Decide-Act".[10] Originally envisioned as an approach for fighter pilots to function in a complex environment while operating within the decision cycles of their adversaries, the concept has been applied to numerous other military, business and other fields at strategic, operational and tactical levels. For example, the National Security Agency, the Department of Homeland Security and the Johns Hopkins University Applied Physics Laboratory borrowed the OODA concept from Col. Boyd as they began looking at automation and orchestration for Integrated Adaptive Cyber Defense. They replaced observing and orienting with sensing and sense-making.

Democratic societies need to examine whether their commonly accepted approaches to sensing and sense-making around political issues and other matters of national interest have evolved alongside technology, media sources and the news cycle. Historically, did individual members of democratic societies outsource their sensing or observation to the media? To what extent has the news media similarly been relied on for sense-making or orientation? As society wrestles with these questions, it can assess the degree to which changes are needed in how the news media and technology are used. This is not to suggest a need to implement hard and fast rules or mandates on the populace. Instead, individuals would simply benefit from self-imposed explorations that improve their awareness of the information sources available to them. How well does an individual know what constitutes news versus opinion, fact versus analysis, trusted versus untrusted information, and—ultimately—foreign-sponsored misinformation?

// Equality sets men apart and weakens them; but the press places a powerful weapon within every man's reach

8 See, e.g., Laura Hautala, "How Microsoft spotted another Russian Hacking Attempt" (August 21, 2018), available at: < https://www.cnet.com/news/how-microsoft-spotted-another-russian-hacking-attempt/>; and see, Reuters, "Facebook, Google and Twitter remove hundreds of accounts from Russia and Iran that tried to influence US elections" (August 22, 2018), available at: < https://www.cnbc.com/2018/08/22/facebook-and-twitter-dismantle-disinformation-campaigns-tied-to-iran-and-russia.html>.

9 Alexis de Tocqueville, Democracy in America, Vol II (New York: Knopf, 1994), p. 324.

10 The OODA Loop concept finds its origins in a paper written by Col. Boyd in 1976. See "Destruction and Creation" in Hammond, A Discourse on Winning and Losing.

For example, it can be quite difficult to distinguish between news segments and opinion segments on mainstream television news media. It once was observed that "[t]he personal opinions of the editors have no weight in the eyes of the public. What they seek in a newspaper is a knowledge of facts, and it is only by altering…those facts that a journalist can contribute to the support of his own views."[11] While that may have been the case during de Tocqueville's experiences in the United States, certainly the consumption of opinion columns increased over the subsequent decades. Nevertheless, it highlights a demarcation between fact and editorial, not to mention false information. But perhaps more relevant in the 19th and 21st centuries is that "[t]he opinions established in the United States under the influence of the liberty of the press are frequently more firmly rooted than those which are formed elsewhere under the sanction of a censor."[12]

And to what extent do individual users of social media understand the algorithms behind the technology they use? Clicking on or "liking" a news story or opinion on many social media platforms will often provide the individual with similar content. P. W. Singer and Emerson Brooking provide a detailed analysis of this phenomenon called "homophily", which they note enables humans to "congregate in such large and like-minded groups. It explains the growth of civilization and cultures. It is also the reason an internet falsehood, once it begins to spread, can rarely be stopped."[13] Although the algorithms and those who deploy them are not nefarious, this pattern can lead to inadvertent compartmentalization of news, opinions, ideas and perceptions that are self-reinforcing and potentially balkanizing. The "coarseness of modern dialogue" can be blamed:

…on the loss of control by old mediators who, whatever their faults and prejudices, operated with an ethos of public service. Replacing them were algorithms designed to keep people on a site, the process driven by a business model where profit was measured by the number of clicks and time spent on a platform.[14]

Foreign influence operations can take advantage of this aspect of social media, which is otherwise designed to assist users in discovering information of interest to them.

Countering such influence operations and ensuring individuals' abilities to build their knowledge and opinions based on ground-truth, while further illuminating that ground-truth through robust public dialogue and debate, is critical to participation in a democratic system of government. Ignoring the internal struggles that emerged within empiricist thought from Locke to Berkeley to Hume and beyond, the Enlightenment principle of "nihil est in intellectu quod non prius fuerit in sensu", or "there is nothing in the understanding that was not earlier in the senses", is important to consider in relation to sensing and sense-making in the modern era of social media.

// An internet falsehood, once it begins to spread, can rarely be stopped

11 de Tocqueville, Vol. I, p. 187.
12 Id., p. 188.
13 Singer and Brooking, p. 123.
14 Michael V. Hayden, The Assault on Intelligence: American National Security in an Age of Lies (New York: Penguin Press, 2018), p. 222. Describing remarks by Zeynep Tufecki at the 2017 Nobel Week Dialogue.

Current democratic institutions were borne of Enlightenment thought. A precondition to successful citizen participation in government is that the populace is sufficiently informed to debate and make governance decisions. The "intellectu" or "understanding" brought to bear on such decisions is constructed based on an individual's opinions and orientations as applied to that which is sensed. Opinions and the factors that influence orientation will differ, but there is a societal benefit from ensuring that individuals have access to true facts, and especially not fabrications designed by a foreign entity to sow discord among a population.

Solutions to this challenge fall within the remit of many. Media outlets and social media platforms can better demarcate news or fact versus opinion and analysis. Local communities, whether government, academic, religious or others, can encourage exploration and consideration of diverse opinions. Governments can increase their transparency and accessibility. But, in the end, individuals need to understand how their opinions are influenced and what they can do to arrive at the OODA Loop decisions and actions best-suited to their personal circumstances.

III. Controlling the Controllable: Confronting Pure Cybersecurity Challenges

While addressing societal adaptation to changes in news media sources and technology will be a long-term endeavor, one opportunity to contest foreign influence operations is considerably more straightforward, immediate and lends itself to the U.S. public-private partnerships already established under a series of presidential policy documents and the National Infrastructure Protection Plan (NIPP). This opportunity focuses on improving the cybersecurity of election infrastructure, political parties, and candidates for public office. Although it does require some investment, the requisite cybersecurity policies, processes, practices and tools are well known. They can be applied to improve the cybersecurity of those entities and people whose information technology systems and data are often targeted by foreign adversaries for purposes of website defacement, political espionage and confidential information harvesting, which can then be used within broader influence operations. This is distinct from efforts to improve the security and resilience of election infrastructure. However, in both cases the Federal government is well-positioned to work alongside State and local election officials, political parties and campaigns, candidates for office and private sector cybersecurity professionals to improve cybersecurity.

GLASSWALL

Specifically related to foreign interference in election infrastructure, efforts of the Department of Homeland Security (DHS) and the FBI demonstrate the commitment to secure that infrastructure. In accordance with the voluntary public-private partnership governance structures established by Presidential Policy Directive 21 and the NIPP, DHS established an election infrastructure subsector government coordinating council, which consists of representatives from DHS, the Election Assistance Commission and 24 State and local election officials, and an industry-led sector coordinating council. These are used to develop partnership activities and plan subsector security and resilience measures that can be taken by government and the private sector. DHS also established an Elections Task Force to coordinate and provide information and cybersecurity services, upon request, to State and local election officials. These services include, among other things, technical assistance, such as cyber hygiene scans, risk and vulnerability assessments, and hunt and incident response assistance. Similarly, the FBI's Foreign Influence Task Force investigates and counters foreign influence operations, engages with private sector companies to share information and threat indicators, and shares information and intelligence with other federal agencies, State and local law enforcement and election officials "to ensure a common understanding of the threat and a unified strategy to address it."[15]

Much has been written about the need to ensure voting machines are air-gapped from other information technology devices and networks. Audit and paper-trail discussions continue among State and local election officials. Similarly, political parties, campaigns and candidates are exploring ways to improve their security to prevent sensitive information from becoming a resource for foreign influence operations. Here, common cybersecurity practices lend themselves to supporting significant improvements in security.

A vulnerability management program, which likely includes vulnerability detection, patch management and other mitigations, can limit the attack surface available to a threat actor. Similarly, configuration management, proper network segmentation, and identity, credential and access management, including two-factor authentication, can prevent or otherwise limit an adversary's abilityto move laterally within an organization.

Individuals and organizations also should consider the use of intrusion prevention systems, next-generation firewalls, antivirus and sandboxing solutions. While some of these solutions will be beyond the capacity of some organizations, they are all good, if not best, practices. At the very least, candidates and their campaigns should enable the security offerings included with their device operating systems or install and regularly update antivirus software. But these security controls are baseline solutions. More is required, and innovations in threat vector mitigation offer tremendous opportunities for broader risk management efforts.

//

Innovations in threat vector mitigation offer tremendous opportunities for broader risk management efforts

[15] FBI, "Combating Foreign Influence" website, available at < https://www.fbi.gov/investigate/counterintelligence/foreign-influence>.

Focusing on the common threat vector of malware delivered via a spear phishing email, organizations looking to mitigate malware risk should consider their defensive postures and how to improve them considering the threat. Generally, email attachments are scanned by traditional, signature-based antivirus solutions at the email gateway and upon execution at enterprise endpoints. Innovations have added heuristic-based antivirus solutions and sandboxing opportunities. Such organizations' success is largely based on prior experience—a combination of previously seen malicious files, malicious behaviors, suspect behaviors, and other attributes of prior attacks. Yet email-based malware continues to effectively compromise individuals and organizations. Increasingly, it is used as a pivot-point from which so-called "file-less" malware can be introduced into an enterprise, presenting its own detection and prevention challenges. And as recently observed, new malware variants were created in 2017 approximately every 4.5 seconds[16] using automated, industrial-scale assembly line malware production approaches and coding malware with the ability to periodically transform itself. This reduces the chance of successful detection and prevention.

Not only are new malware variants proliferating, but threat actors continue to use file-based malware in email spear phishing campaigns. These include nation state actors, criminal groups and others. Table 1 provides a snapshot of just some actor groups whose tactics, techniques and procedures include the use of malicious formatted files in spear phishing campaigns. While these groups are continuously evolving their arsenals of intrusion techniques, it is not surprising that they often return to the effective method of spear phishing with malicious files attached or linked to the email considering the success this approach carries. One can only conclude that while detection is necessary for effective cybersecurity, it is not sufficient. The "SANS 2018 Survey on Endpoint Protection and Response" suggests that "[t]raditional tools are no longer sufficient to detect cyberattacks, the data shows: Antivirus systems only detected endpoint compromise 47% of the time," and that advanced behavior-based detection tools are being purchased, but not used due to lack of training and bandwidth among already over-worked information security teams.[17]

Actor Group	Initial Access Vector	Execution	Targets
APT 28	Spearphishing with Attachment	Excel with macros; Word with DDE execution	U.S. government; election infrastructure
APT 29	Spearphishing with Attachment; Spearphishing with Link	Word; PDF; other tailored attachments;	Governments in the U.S., Europe, Central Asia, East Africa and the Middle East; election infrastructure
APT 37	Spearphishing with Attachment	Office files exploiting CVE-2017-0199; DDE links to execute VBS	Various verticals, including chemicals, electronics, manufacturing, aerospace, automotive and healthcare, primarily in South Korea, Japan, Vietnam and the Middle East
APT 10	Spearphishing with Attachment	Disguised executables; Excel	Healthcare, defense, aerospace, mining, IT service providers and government, primarily in Japan
Leviathan	Spearphishing with Attachment; Spearphishing with Link	Excel and Word with macros; malicious Publisher files	Defense and government as well as engineering, maritime, manufacturing and universities in U.S., Europe and South China Sea region
Sneaky Panda	Spearphishing with Attachment; Spearphishing with Link	Multiple file types	Defense, maritime, IT services, supply chain, energy, and aerospace sectors.
APT 33	Spearphishing with Link	.hta file links	Targets the U.S., Saudi Arabia and South Korea with particular interest in the aviation and energy sectors
APT 35	Spearphishing with Attachment; Spearphishing with Link	Excel and Word with macros	Government, IT and energy sectors with a nexus to Saudi Arabia
OilRig	Spearphishing with Attachment	Excel and Word with macros	Primarily focused operations in the Middle East; also uses supply chain trust relationships
FIN 7	Spearphishing with Attachment	Word with DDE execution	Financially-motivated with primary focus on the retail and hospitality sectors
FIN 8	Spearphishing with Attachment; Spearphishing with Link	Word with macros	Financially-motivated with primary focus on the retail, hospitality and restaurant sectors

Table 1 - Sourced from compiled information available in MITRE's Group List (https://attack.mitre.org/wiki/Groups)

16 G Data Security Blog, "Malware Numbers 2017" (March 27, 2018). Available at: < https://www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017>.

17 Kelly Sheridan, "Less Than Half of Cyberattacks Detected via Antivirus: SANS", dated July 16, 2018. Summarizing the SANS 2018 report and available at: <https://www.darkreading.com/endpoint/less-than-half-of-cyberattacks-detected-via-antivirus-sans/d/d-id/1332309?_mc=NL_DR_EDT_DR_weekly_20180719&cid=NL_DR_EDT_DR_weekly_20180719&elq_mid=85822&elq_cid=25863258>.

GLASSWALL

IV. Innovative Cybersecurity Is Available Now

For too long, the cybersecurity community has been trying to solve an increasingly intractable problem—identifying and stopping malicious file attachments before they infect an endpoint or network. Yet, automated assembly-line ransomware generation on an industrial scale, coupled with sandbox-aware or at least sandbox-evading attributes, will continue to defeat detection approaches far too often. The end goal of preventing malicious files from infecting an enterprise remains sound, but it requires solving a simpler problem. Instead of detecting and preventing "known-bad" files, enterprise email security must incorporate technology to simply look for, generate and pass "known-good" files.

Generating and passing "known-good" files can be achieved using deep-file inspection, remediation and sanitization technology (d-FIRST™), which has been maturing for several years and is already available in the cybersecurity marketplace. Glasswall FileTrust™ Advanced Threat Protection is just such a technology. In near real-time, it will compare a file to that file type's standard or specification (e.g., Microsoft Office specifications, ISO 10918 for JPEG, ISO 32000 for a PDF file), regenerate the file in accordance with that specification, and pass the file forward. During the regeneration process, Glasswall FileTrust™ performs two sets of actions. First, it remediates structural deviations from the file type specification. This includes fixing byte-level anomalies, which may be intentionally or unintentionally introduced into the file but can create unwanted consequences. Second, it sanitizes functional aspects of the file based on an enterprise's security policies. For example, it can remove extensible attributes, such as macros, JavaScript, embedded files and metadata. Sanitization can be applied differently depending on user groups and their business needs.

The d-FIRST™ approach is a departure from traditional security techniques; more to the point, it's approach is the opposite of all preceding security solutions. All files are subjected to the process on a least-trust basis, instead of only acting on files that match a known signature or heuristic pattern. The results, however, fill a gap in traditional architectures. For instance, Glasswall Solutions tested 6,000 known and unknown malicious files with a global defense contractor. Initially, only an antivirus solution was deployed. Of the 6,000 malicious files, 3,592 of the files were detected by the antivirus solution—a 40.13% failure rate. Subsequently, a heuristic layer was added by the systems integrator, which reduced the failure rate to 35.58%. Finally, Glasswall FileTrust™ was inserted in place of the signature- and heuristics-based solutions. Each of the 6,000 files was effectively remediated and sanitized because Glasswall FileTrust™ was not looking for known-bad.

GLASSWALL

In an operational example, a well-known brand that is a Glasswall Solutions customer in the information technology sector received 347 million emails over a six-month period, which included Microsoft Office, PDF and image files. Four layers of defense were applied to the files, including next generation firewalls, anti-spam and anti-phishing filters, antivirus solutions and a heuristics filter. Fifty-five million of the original files were allowed to pass as "clean" to Glasswall FileTrust™, the company's final line of defense prior to the email server. The multiple security layers failed to prevent 171 malicious files, almost an average of one file per day. According to the customer, Glasswall FileTrust™ neutralized the threats with no impact to the end-user experience. Glasswall Solutions began querying well-known malware repositories with the hashes of the original 171 malicious files. In some cases, the malware was known to the antivirus community, but the traditional solutions lacked a matching signature and did not interdict those files, similarly, the sandbox layer had been bypassed using new and previously unseen techniques. In other instances, not only did Glasswall FileTrust™ protect the customer on day-zero, but it took up to three, seven and even 30 days for the antivirus community to indicate awareness of the malicious files, and longer for the sandbox vendor to develop, test and release its updated software. Of course, with the d-FIRST™ approach this is to be expected. By subjecting all files to the security solution, previously unknown malware will be rendered inert. Customers are not only protected by Glasswall FileTrust™ on day-zero, but they have access to personalized threat intelligence as these are files often specifically directed towards them.

//

Glasswall FileTrust™ neutralized the threats with no impact to the end-user experience

GLASSWALL

V. Conclusion

The principles upon which democratic societies are founded include an informed populace. This is a key enabler of democratic institutions such as citizen participation in government through free and fair elections, support for the rule of law, concern for civil rights and liberties, and oversight of those who govern. While government has a role in protecting democratic institutions from foreign interference, individual citizens, organizations and society must collectively do more to ensure an expansion of knowledge based on truth, which will enable informed debate over a variety of more and less contentious issues.

When it comes to the sanctity of elections, assurance of an informed populace is essential. Foreign influence operations must be identified and prevented. Where that is not possible, resilience to the operations' intended effects must be constructed. Government may take a secondary role in this space, but it, the private sector, political campaigns and candidates for office each have primary roles to play in effecting better security around voting infrastructure and systems and data that could be exploited as part of a foreign influence operation. Cybersecurity best practices, along with the tools, processes and people to implement them, are available. At the same time, stagnation is not an option—innovative solutions that represent new and emergent practices are necessary to address dynamic and innovative threat actors.

One such emergent practice is the use of technologies that convert formatted files into "known-good" states instead of attempting to detect and prevent "known-bad" files from entering an enterprise. Glasswall Solutions can support an organization's effort to introduce innovative cybersecurity solutions through a no-cost risk assessment, which will demonstrate current security gaps and exposures as they relate to the formatted files entering and exiting the enterprise.

GLASSWALL

UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652
cdssales@glasswallsolutions.com
glasswallsolutions.com
Glasswall Solutions limited
@glasswallnews