CohnReznick ADVISORY • ASSURANCE • TAX | esentire®

THREAT REPORT REVEALS BROADENED ATTACK ATTEMPTS

October 2018

This year is shaping up to be another banner year for cybercriminals. During the first six months alone, a staggering 4.5 billion data files were breached, a 133% increase over the same period in 2017.[1]

Most of these intrusions are perpetrated by external threat actors who exploit IT technologies and internal users to gain access to systems, applications, and data. In working with businesses over the past year, CohnReznick has seen an increase in web server intrusions and compromises primarily caused by malware being implanted on systems via phishing attacks.

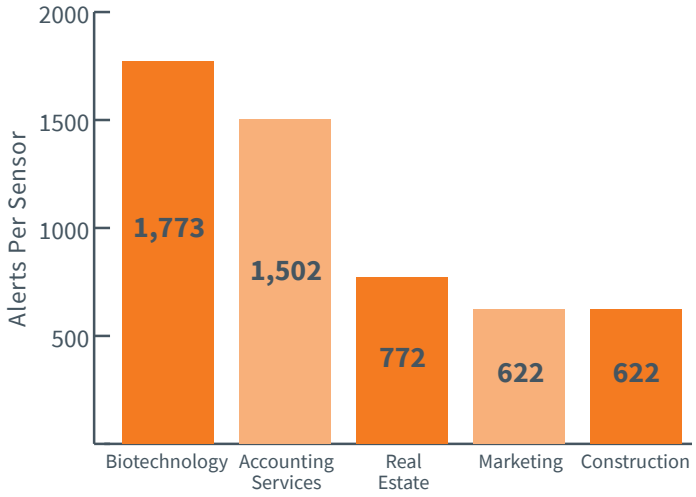
Our work in the field is corroborated by a new threat report published by eSentire, a service provider that combats cyber threats. The report reveals a massive proliferation of attacks on web technologies through unpatched vulnerabilities and computers via PowerShell exploitations and phishing campaigns. The *Q2 2018 Quarterly Threat Report* is drawn from 57,000 security alerts investigated by eSentire's Security Operations Center during the second quarter of 2018.

The report found a stunning spike in intrusion attempts on Microsoft's web servers, compared with the first quarter of 2018. Attacks on Microsoft's web servers skyrocketed from 2,000 in Q1 to 1.7 million in Q2, a 782-fold increase. In addition to Microsoft's web servers, eSentire also noted an uptick in intrusion attempts against Drupal and Oracle WebLogic web technologies. These types of compromises can enable cybercriminals to remotely control and execute malware on web servers, causing potential theft or corruption of data or degradation of system's uptime.

Among our clients, attacks on web servers have occurred when businesses fail to patch or upgrade operating systems and applications. Adding to the potential threats and vulnerabilities, many organizations lack secure coding and configuration practices to prevent malware from entering a company's publicly accessible application.

Our cybersecurity teams also have encountered a comparatively new threat: Cryptojacking, which occurs when a cybercriminal maliciously uses a computer's processing power to mine for Bitcoins or other cryptocurrencies. The effect of this exploit may dramatically degrade performance and availability of the attacked system.

Top 5 Industries Experiencing Verified Hostile Traffic



Source: eSentire, Q2 2018 Quarterly Threat Report, September 2018

POWERFUL POWERSHELL EXPLOITS

Beyond web technologies, the eSentire report identified a 50% increase in PowerShell exploits. Cybercriminals often manipulate PowerShell to hide malware that they have implanted on IT systems. eSentire ties an increase in the malware, Emotet, which utilizes unauthorized PowerShell commands to perform its attacks.

In our experience, PowerShell compromises are often a result of insecure configurations and ineffective security controls. We advise businesses to limit those who can initiate PowerShell commands to only necessary users. It's also critical to continuously log PowerShell changes and implement notification capabilities to alert administrators when suspicious PowerShell commands are executed.

[1]Gemalto, Breach Level Index: 2018 First Half Review, September 2018

A BROADER NET FOR PHISHING EXPEDITIONS

While phishing is nothing new, the intrusion technique continues to evolve. eSentire found specific shifts in the types of lures used to persuade email recipients to click links or open documents.

Lures that emulate email from shipping companies such as UPS and FedEx, as well as eFax services, increased significantly. Particularly striking was a 100% hike in phishing campaigns that mimic UPS email messages. On the other hand, eSentire found that phishing attempts using internet service lures like Google and Dropbox significantly declined as more threat actors shifted to HTTPS techniques.

Among our clients, one of the most effective lures is a fraudulent request for wire transfers, a compromise using targeted spear-phishing attacks. Cybercriminals typically impersonate business executives who have the authority to approve wire transfers, and ask finance employees to initiate the transaction. To combat spear-phishing attacks or campaigns, organizations will need to update email applications and spam filters to help identify and stop malware-laden messages. We also recommend that businesses lock down their workstations by only allowing approved applications to be installed.

It's also important to regularly conduct employee security awareness training for specific threats like phishing and suspicious emails appearing to come from known parties. We work with clients to develop training programs that test employee awareness, by sending a seemingly legitimate email to employees and executives, and then share the results of which emails most successfully tricked people. This exercise helps employees understand how to identify and avoid future phishing attempts.

Finally, it's critical to include governance as a pillar of your cybersecurity program. You should provide ongoing threat and risk intelligence to top executives and board members, so they have the information needed to uphold their fiduciary obligations. Good governance also enables leadership to set a culture of security that focuses on identifying threats and suspicious activity across the enterprise.

TAKE STEPS TO SAFEGUARD YOUR DIGITAL ASSETS

The right cybersecurity safeguards can help you curb intrusion attempts and limit the impact of malware and other potential threats. The following technologies, processes, and people skills can help you protect your digital assets:

- Regularly patch and update applications, and operating systems
- Employ the principal of "least privileged access" to limit the access rights of groups or individuals to only perform necessary functions on their devices or workstations
- Restrict administrative privileges to appropriate administrative personnel
- Do not give users administrative rights to PowerShell
- Update spam filters to help identify new threats
- Implement reputation blocks to limit user access to potentially harmful websites
- Lock down workstations to prevent installation of malware
- Use email security configurations to block known malware from spam
- Conduct employee security awareness training for overall best practices as well as specific threats like phishing and suspicious email behaviors from known parties

CONTACT

For more information about how CohnReznick and eSentire can help with your cybersecurity program, contact:

Shahryar Shaghaghi
Principal
CohnReznick Advisory
646.601.7899
shahryar.shaghaghi@cohnreznick.com

Tim Horigan
Field Channel Manager
eSentire
716.870.6040
Tim.Horigan@esentire.com

About eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.eSentire.com and follow @eSentire.

About CohnReznick

CohnReznick LLP is one of the top accounting, tax, and advisory firms in the United States, combining the deep resources of a national firm with the hands-on, agile approach that today's dynamic business environment demands. With diverse industry expertise, the Firm provides companies with the insight and experience to help them break through and seize growth opportunities. The Firm, with origins dating back to 1919, is headquartered in New York, NY with 2,700 employees in offices nationwide. CohnReznick is a member of Nexia International, a global network of independent accountancy, tax, and business advisors. For more information, visit **www.cohnreznick.com**.