THINK APP SECURITY FIRST

THE EVOLVING RISK LANDSCAPE

PREPARING FOR EMERGENT THREATS

INTRODUCTION

In today's digital marketplace, your applications are your business.

They fuel innovation and are the driving force for staying competitive in an always-on, always-connected world. Apps are the way you build relationships with your customers, empower your employees, facilitate growth, and so much more.

The rise of the cloud has produced billions of new apps that hold untold amounts of confidential data. These cloud-based apps give businesses of all sizes the agility necessary to thrive in an increasingly fast-paced marketplace. However, they also create a host of complex challenges—and new risks. And, with automated tools and a growing repository of expertise for hire, threats are increasing and hacking has turned into a for-profit game.

So, while apps have increased productivity and the speed of innovation, they have also opened the door to unprecedented threats, expanding the risk landscape and putting corporate data and reputations at risk.

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

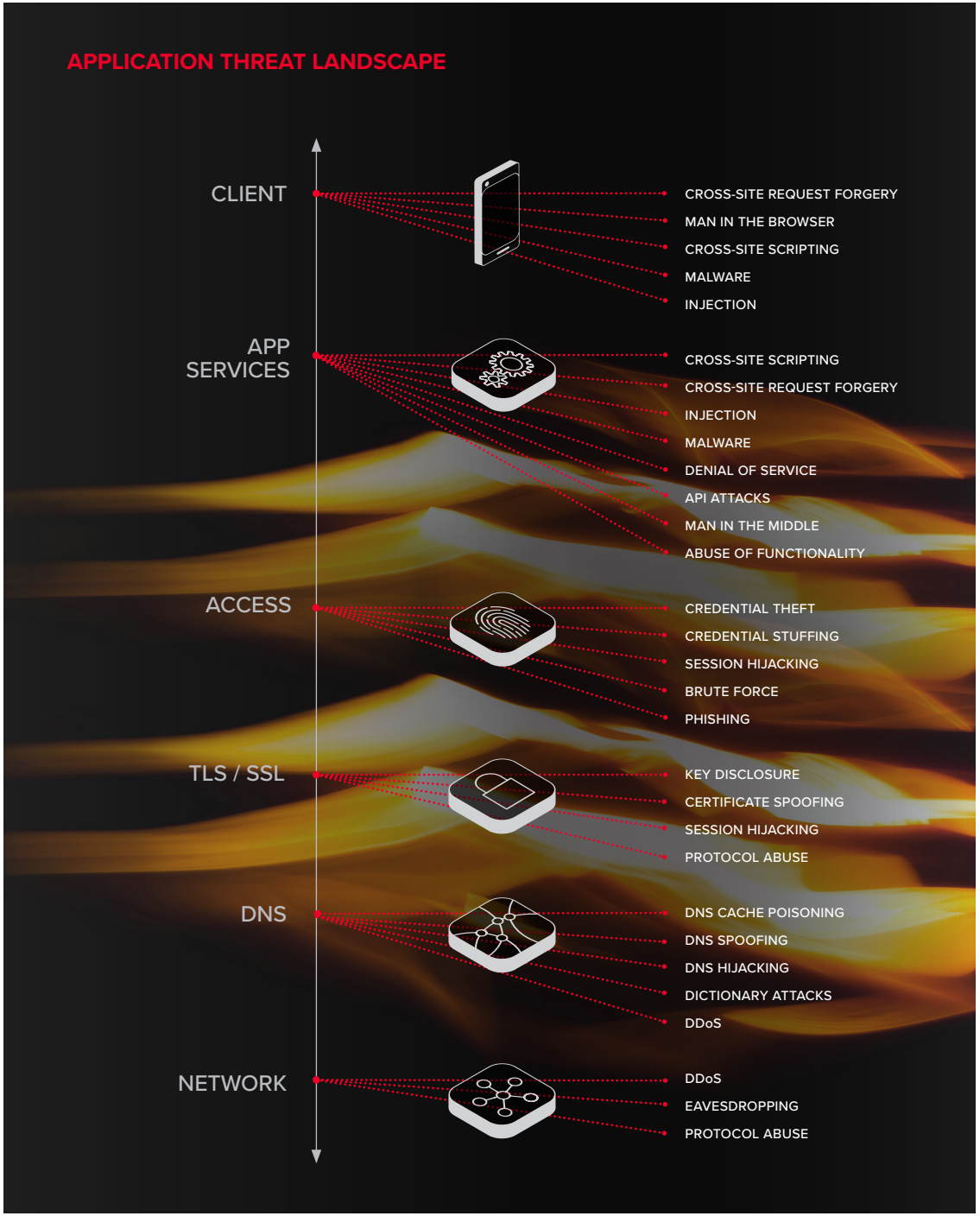
ACCELERATING YOUR BUSINESS

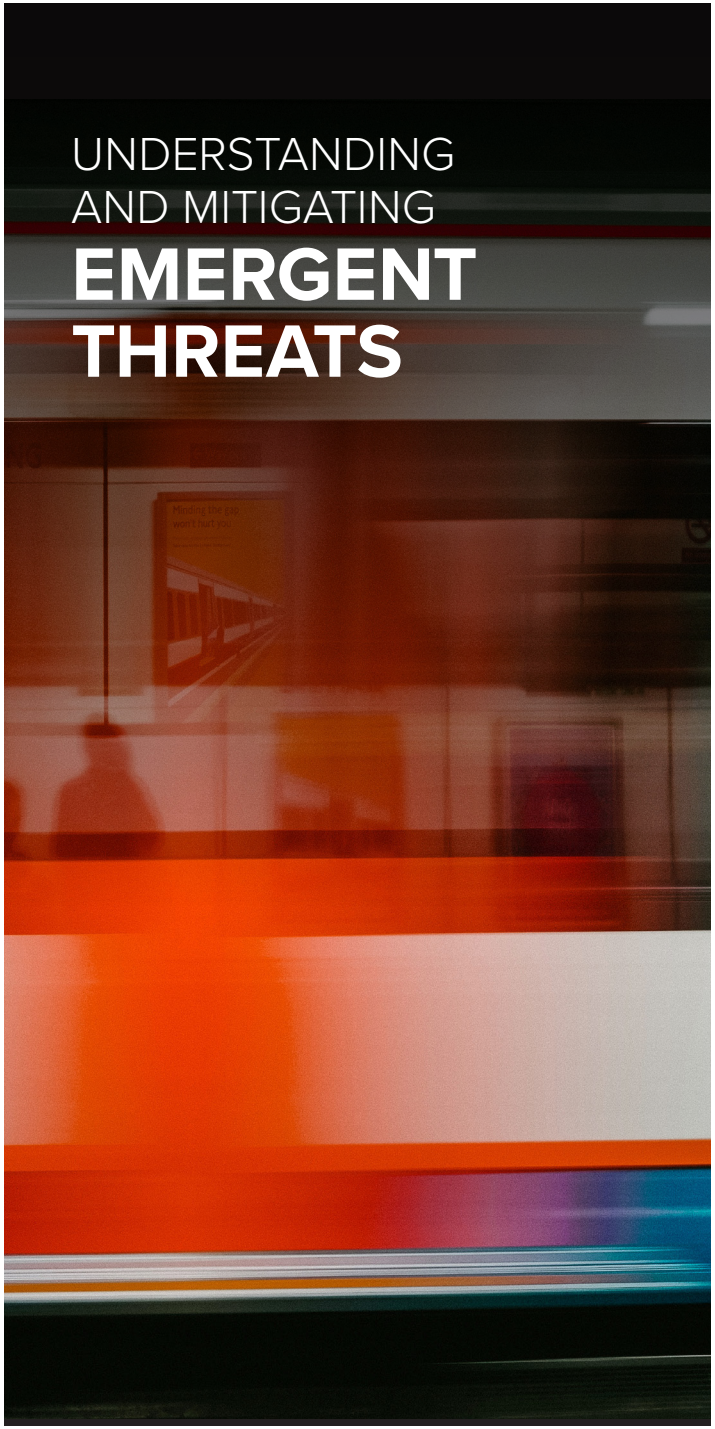
MEANS SECURING YOUR APPS

In such a complex landscape of threats and opportunities, balancing innovation and security can feel like an unwinnable battle. But it doesn't have to be that way. Organizations must ask themselves where they should allocate security dollars to provide the strongest level of protection for the business.

Understanding the application itself—and its key areas of vulnerability—is a critical starting point. Organizations should consider the network the app resides on; the data that travels from the user to the app; the DNS that resolves the IP address to access the app, the web and application servers; and the associated APIs that are leveraged by other applications and systems.

It's essential to leverage threat intelligence to recognize today's most critical threats to your application—whether the app is the primary target or a secondary factor for launching larger-scale attacks (think IOT botnets). Staying abreast of new attack vectors and tactics can deepen your understanding of the threat landscape and give you actionable information to help keep your apps and your organization safer. With this knowledge, you can adopt solutions that will best serve your business, protecting against threats at all entry points of app vulnerability so you can better ensure the confidentiality, integrity, and availability of your apps and your data.





WEB FRAUD

Web fraud is primarily associated with the banking industry—and, indeed, financial services companies experience the most attacks because they have the highest-profile assets. However, businesses in all industries are at risk of web fraud, which is a multifaceted threat that costs organizations billions of dollars a year. It can take the form of bots that help scalpers acquire and then resell in-demand items like limited-edition shoes, tickets to popular events, and even government visas.

- E-commerce fraud rose 33% in 2016.[2]
- Cybercriminals take aim at bank accounts, rewards programs (like frequent flier miles), credit cards, and other private information such as medical records that can be used or sold for financial gain.
- Web fraud even affects the integrity of online information as content scrapers steal and re-publish content.
- Web fraud can also negatively impact your brand and consumer perception of your business since product availability and pricing competitiveness may drive customers to competitors.

SOLUTION

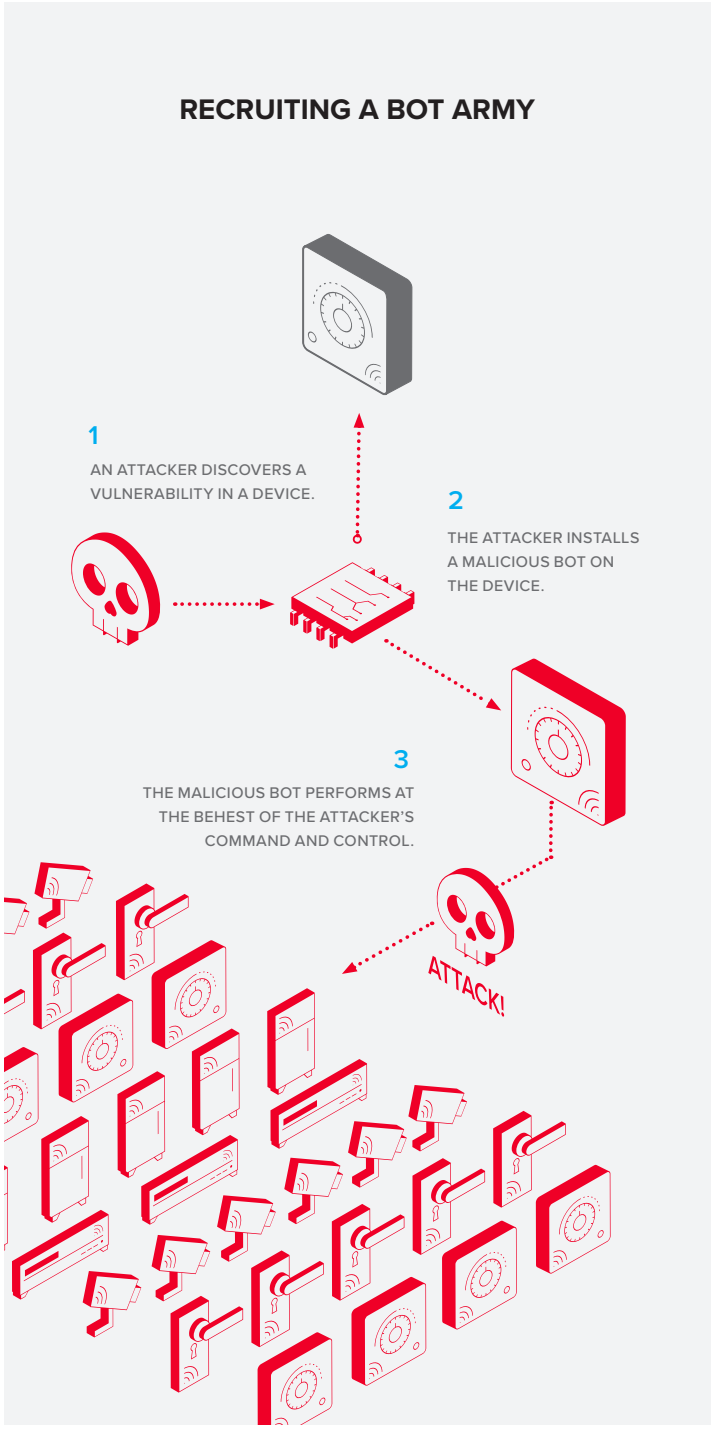
Minimizing the attack surface for web fraud involves a combination of human and machine efforts to identify and protect against financial and in-browser malware, zero-day fraud, and other fraudulent online activities.

33%

E-COMMERCE FRAUD ROSE 33% IN 2016.

- Leverage advanced identification techniques to enable your organization to recognize and be informed of malware patterns, including injections of malicious scripts, attempted automated transfers, and remote access trojans/malware that give attackers administrative control over a victim's computers.
- Adopt anti-fraud solutions that can detect and prevent automated payments and money transfers initiated by malware or bots by assessing a variety of device-specific and behavioral variables, which together are designed to distinguish human users from automated scripts or bots.
- Since bots are so frequently associated with fraud, deploy bot mitigation and management solutions to deter and manage fraud-related problems.
- Review in-depth analysis of business processes as they can reveal areas of weakness that could be exploited for financial gain.

[2] http://www.experian.com/blogs/insights/2017/03/e-commerce-fraud-rates-spike-in-2016/



BOTS

In 2016, more than half of the online traffic was initiated by software and not humans.[3] The rise of bots—both good and bad—has changed the nature of the Internet as we've known it. From the infamous DDoS attacks from the Mirai botnet[4] to web-scraping bots, spam bots, scalper bots, and credential stuffing bots, the automated applications taking over the Internet have earned a bad reputation. Much of that is warranted, as bots of all varieties can have varying impacts on legitimate sites, and are often the weapons used by attackers. They are also frequently associated with business intelligence gathering (such as pricing data), which allows competitors to undercut others in their respective industries.

- Botnet activity accounted for 77% of breaches in 2016.[5]
- Spammers used 100,000 IoT devices to send out three-quarters of a million emails.[6]
- A crypto-currency mining IoT worm compromised over 30,000 computers and devices in four months.[7]

However, not all bots are bad bots. Many bots work on behalf of legitimate users or for legitimate purposes, such as personal digital assistants, spider bots indexing the web, or copyright bots sniffing out plagiarized content. As the Internet becomes more and more the realm of bots, organizations must develop and deploy strong mechanisms to identify, classify, and defeat the bad bots, but they will also need the intelligence, context, and relationships that allow them to aid—or at least not hinder—the bots working for legitimate purposes.

SOLUTION

Protecting your organization from the malicious bots on the Internet requires advanced and proactive bot-detection capabilities, which allow you to identify suspicious automated activity, categorize bots detected, and mitigate attacks with a high level of precision.

- Incorporate highly programmable traffic management solutions that dynamically adapt policies and proactively stop bots to optimize processes and make the best use of your security team's time.
- Protect against automated DoS attacks, web scraping, and brute force attacks before they occur with always-on defense.
- Use advanced defense methods (such as JS and CAPTCHA challenges) and reputation matching to identify non-human users.
- Implement systems that can leverage threat intelligence feeds, such as IP intelligence, to automatically block bot-hosting endpoints at L3.
- Test your web applications to find potential vulnerabilities.
- Use multifactor authentication to make it difficult for bots to gain access to your applications and network.
- Minimize risk by limiting the amount of personal information stored in your web applications.
- Determine the likelihood of becoming the target of a given threat actor or attack campaign by using actionable threat intelligence.

[3] https://www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference

[4] https://f5.com/labs/articles/threat-intelligence/ddos/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-attack-on-ovh-22422

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[6] http://www.dailytech.com/Hackers+Use+Refrigerator+Other+Devices+to+Send+750000+Spam+Emails+/article34161.htm

[7] https://www.symantec.com/connect/blogs/iot-worm-used-mine-crypto-currency

CREDENTIAL STUFFING

In a credential stuffing attack, cybercriminals use stolen login usernames and passwords to make repeated attempts to gain access to accounts held by corporate users or customers. With the number of data breaches growing every year, more and more credentials are being exposed. And with the average set of usernames and passwords selling for more than 17 times the price of a stolen credit card number, credential theft is a booming business.[8] While credential stuffing is largely a consumer problem, password reuse among accounts could put corporate accounts at risk, too.

- In the first six months of 2017, there were 2,227 breaches reported, exposing over 6 billion records.[9]
- Three out of four users reuse and recycle credentials across accounts.[10]
- Credentials stolen from customers are the predominant method of web application compromise.[11]

The bottom line is that no matter how strong your organizational security is, if your users or customers reuse passwords, then the likelihood is that their credentials have already been stolen and made available for sale on the dark web.

SOLUTION

While there's no silver bullet for the problem of credential stuffing, you can protect your organization with a combination of training your employees/users and bolstering your own defenses.

- Help employees protect themselves against credential theft by boosting security awareness about phishing with training and education.
- Provide advanced bot detection and prevention with a web application firewall, which is key because most credential stuffing attacks are launched using automated programs.
- Design your site's login form so that it is impossible for the attacker's bot to recognize the correct fields and insert the stolen credentials with dynamic form obfuscation.
- Ensure that data in the browser or your mobile apps is encrypted to protect the information transferred from users and render any intercepted data worthless.
- Decrease risk by leveraging single sign-on (SSO) and risk-based multifactor authentication through a centralized access gateway.
- Limit liability by enabling federated authentication for users, which has the added bonus of not requiring them to manage yet another password.
- Monitor for failed authentication attempts and classify their sources in order to help identify and block malicious endpoints.

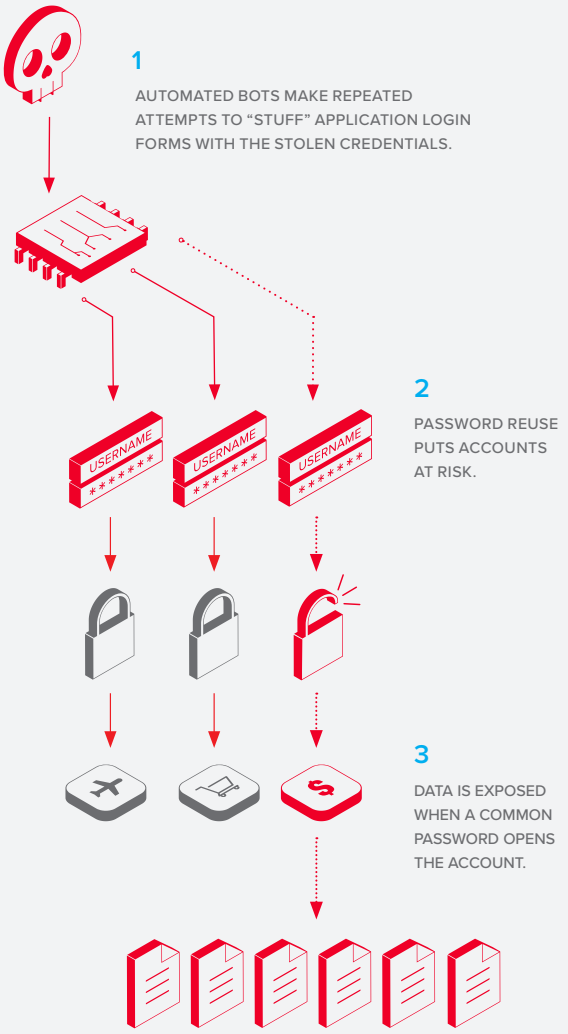
[8] http://www.darkreading.com/endpoint/anatomy-of-an-account-take-over-attack/a/d-id/1324409

[9] http://www.securityweek.com/2227-breaches-exposed-6-billion-records-first-half-2017-report

[10] https://www.entrepreneur.com/article/246902

[11] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

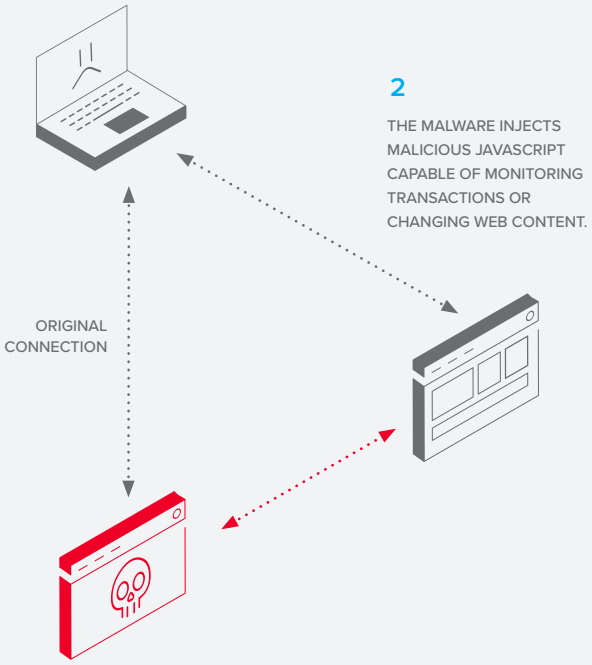
ANATOMY OF A CREDENTIAL STUFFING ATTACK



MALWARE EXAMPLE

1

A USER INFECTED WITH MALWARE BROWSES A SITE. THE MALWARE RECOGNIZES THE URL AS ONE IT WANTS TO STEAL CREDENTIALS FROM.



MALWARE

From trojans and viruses to adware and rootkits, malware is ubiquitous. It's used for anything and everything, including web fraud, credential theft, and the construction of botnets that conduct DDoS attacks. While malware is incredibly diverse, it's all designed to facilitate the end goal of the attacker, which could include financial gain, enrollment of a device in a botnet, propagation of spam, or account takeover. The key to managing risk for malware is understanding the risk profile for your industry as well as the types of malware being employed by common threat actors.

- In the first quarter of 2017, a new specimen of malware emerged every 4.2 seconds.[12]
- Over half (51%) of all breaches in 2016 involved some form of malware.[13]

SOLUTION

Traditional solutions for malware such as antivirus programs and blacklisting software packages are simply not effective enough against the proliferation of trojans, spyware, adware, and more. To best protect your organization against malware, it's essential to employ a combination of behavioral analysis and threat intelligence.

- Prevent malware from executing with application whitelisting.
- Assess software with behavioral analysis, which examines how a piece of software acts—not just its file signature.

66%

OF MALWARE WAS INSTALLED VIA MALICIOUS EMAIL ATTACHMENTS.[14]

- Protect the user's system and network with sandboxing, which forces attachments or links to open in an isolated execution environment.
- Restrict permissions so that most users don't have the opportunity to install software, which can increase the burden on IT, but will help contain the spread of malware.
- Help users discern scams and differentiate legitimate sites and services from those intended to facilitate malware distribution.
- Maintain an easily accessible library of known good software for users to enable them to get things done faster with less risk to the network.

[12] https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017

[13] https://www.gdatasoftware.com/blog/2017/04/29666-malware-trends-2017

[14] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

RANSOMWARE

Ransomware is a type of malware that prevents users from accessing their own data and computers by locking their screens or encrypting files. It has become increasingly popular over the past few years, most notably in the public administration, healthcare, and financial sectors.

In fact, it moved from number 22 on the list of most popular malware in the 2014 Verizon Data Breach Investigations Report to number 5 in 2016.[15] By locking out users or encrypting certain files on their system, attackers attempt to extort payments from them.

- Ransomware is notably opportunistic, relying on downloads and phishing attempts to compromise systems.
- Over the past year, attackers have begun targeting vulnerable organizations in addition to consumers in an attempt to ramp up revenue.[16]
- Cybercriminals now offer ransomware-as-a-service, taking a cut of any payments made by users or organizations.[17]
- In a recent study, ransomware bypassed traditional antivirus 100% of the time.[18]

SOLUTION

Earlier detection of ransomware attacks combined with threat intelligence can help bring cybercriminals' efforts under control.

- Use endpoint protection systems to detect common ransomware samples and block them before they can affect the network.
- Educate users about phishing attempts, which are one of the main ways ransomware is introduced into a system.
- Empower your system to block unidentified applications from being installed or executed with application whitelisting.
- Share threat intelligence to help stop the spread of ransomware.

[15] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[16] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

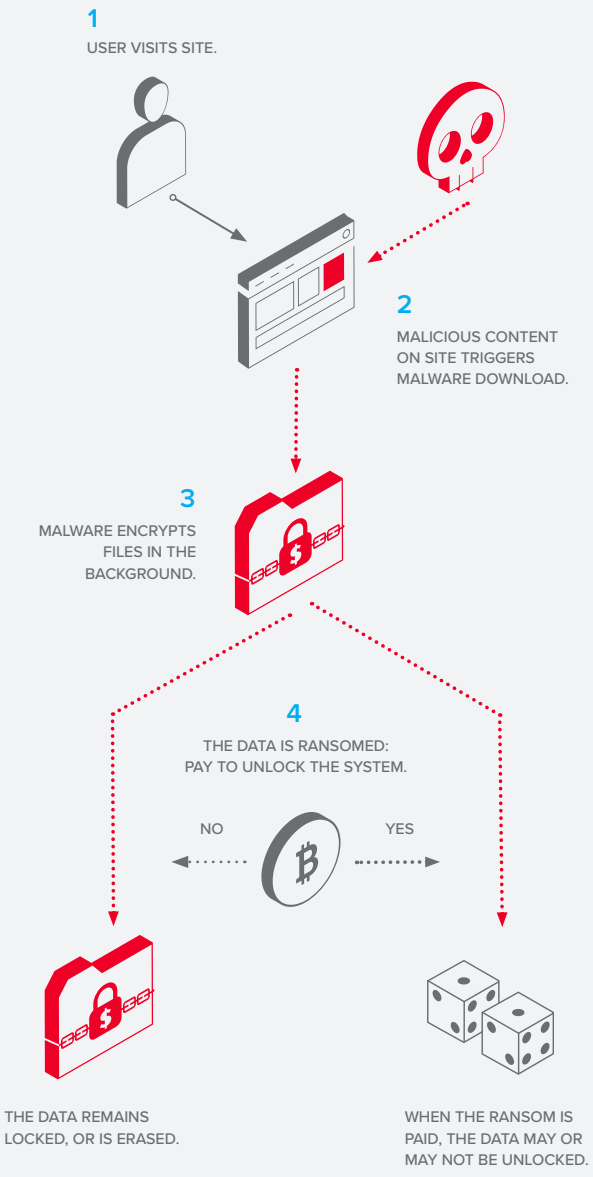
[17] https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#2f19d94e4123

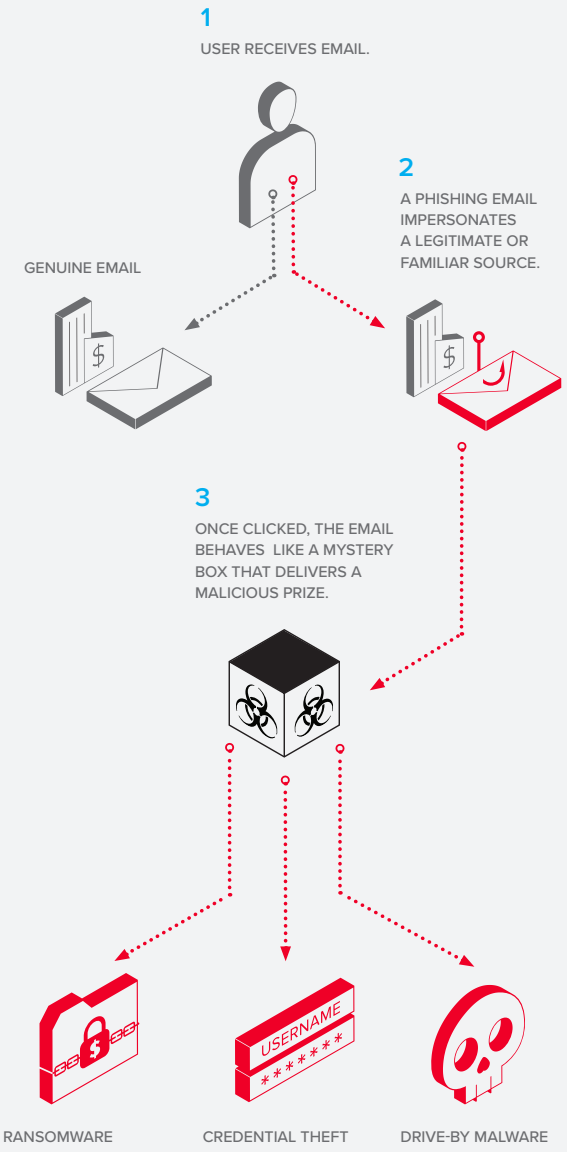
[18] https://www.infosecurity-magazine.com/news/antivirus-fails-to-stop-ransomware/

100%

IN A RECENT STUDY, RANSOMWARE BYPASSED TRADITIONAL ANTIVIRUS 100% OF THE TIME.

RANSOMWARE DATA LOCK-UP





PHISHING

Like many of these threats, phishing doesn't fit easily into one category—it is most often a means to another end. Attackers use phishing scams to trick users into clicking on a link that can infect their system with malware or take them to a fake website designed to steal personal information.

Phishing can help cybercriminals take over users' accounts, gain access to confidential data, and steal money or other commodities such as frequent flier miles. In addition, it's common in phishing attacks to trick users into installing command-and-control malware on their systems, which can provide backdoors into corporate networks.

- Phishing is the primary delivery mechanism for ransomware and other types of malware.[19]
- No industry is immune to phishing attacks, and the percentage of users who end up clicking on phishing links is largely the same across verticals.[20]
- An increase in phishing attempts may be a precursor to an advanced persistent threat campaign; actionable threat intelligence can help identify and associate a seemingly smaller problem with a larger or longer-term attack.

ENCOURAGE USERS TO REPORT SUSPICIOUS EMAILS, OR ALERT THE ORGANIZATION IF THEY DO CLICK ON A PHISHING LINK.

SOLUTION

There's no single solution that will stop phishing attacks; instead, organizations must train their users—and keep training them—in how to spot phishing emails, and what to do if they click on one by mistake.

- Conduct security awareness training to help your employees and contractors stay abreast of emerging phishing attacks.
- Set up policies that make it easy for users to report an incident to IT immediately if they think they've clicked on a malware link in a phishing email or have mistakenly divulged their credentials.
- Detect and stop malware with strong endpoint protection mechanisms.
- Encourage users to report suspicious emails.
- Develop a simple process for users to alert the organization if they do click on a phishing link.
- Use threat intelligence to calculate the likelihood of your company becoming the target of an advanced persistent threat campaign that may attempt to leverage phishing to infiltrate your systems.

[19] https://blog.barkly.com/phishing-statistics-2016
[20] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

NEW VULNERABILITIES
NEW OPPORTUNITIES

In this rapidly changing app-centric world, complexity is the order of the day. The days of siloed threats mitigated by point solutions are long gone. Your applications are holistic, so you need a holistic approach to protect them.

With apps being delivered from anywhere and everywhere—including data centers, private clouds, public clouds, containers, SaaS platforms, and more—adopting an integrated approach to security is critical to protecting your infrastructure, your applications, and your data.

By carefully considering current and emerging threats, utilizing and sharing threat intelligence, and aligning solutions with budget requirements, you can build out a comprehensive security program that helps your organization be successful—and safe—both now and in the future.

For more information on the threats that affect your organization, and what you can do to defend against them, visit f5.com/security.

THINK APP SECURITY FIRST

Always-on, always-connected apps can help power and transform your business–but they can also act as gateways to data beyond the protections of your firewalls. With most attacks happening at the app level, protecting the capabilities that drive your business means protecting the apps that make them happen.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com