How to Avoid Falling Prey to Ransomware

What small, midsize and distributed enterprises need to know about the advanced malware attack plaguing businesses and capturing news headlines around the world

WatchGuard®

WHAT IS RANSOMWARE?

Ransomware is a form of computer malware that disables your access to your computer or the information within it through encryption, while demanding you pay a ransom to receive the decryption key to regain access.

WHY DOES IT MATTER TO ME?

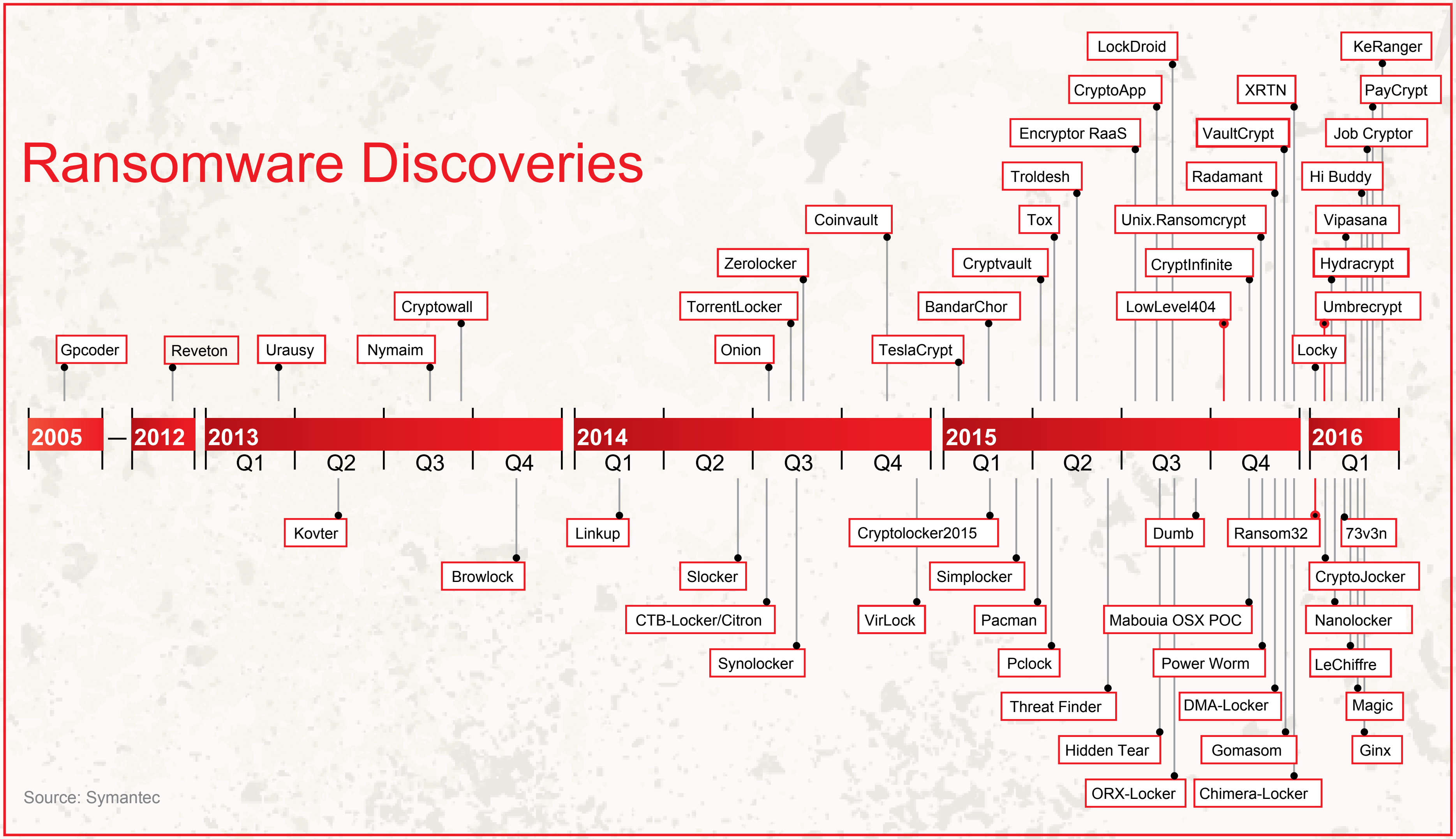
Reports indicate that 42% of small and midsize businesses (SMBs) consider crypto-malware (such as ransomware) to be one of the most serious threats they face – and for good reason! Ransomware attacks are becoming increasingly focused on SMBs and distributed enterprises where they find a large number of organizations with network security that is often insufficient to detect and prevent known advanced malware. Cyber criminals often view SMBs and distributed enterprises as "low hanging fruit!" **While the ransom requested is usually around $300, research shows that on average a single ransomware attack could cost small and midsize businesses up to $99,000[1].**

In this eBook, we'll explore some key trends we are seeing in the ransomware threat – and provide strategies and best practices to defend against these attacks.

42% of SMBs consider crypto-malware to be THE MOST SERIOUS threat they face.[2]

RANSOMWARE COMES OF AGE

Ransomware is an increasingly common method of attack for hackers against individuals, SMBs and enterprises alike. While the first incidents of ransomware were discovered in as early as 2005, the last three years have seen this type of threat explode in popularity and compromise millions of computers and mobile devices around the world.



Ransomware Discoveries

Source: Symantec

RANSOMWARE FLIPS THE SCRIPT

In security we often talk about the need to protect data that is sensitive and keep it out of the hands of attackers who could use that data for their own gain. We've seen massive breaches of public and private organizations that have resulted in huge financial loss as the result of criminals using stolen personally identifiable information (PII) and credit card numbers to perpetrate further crimes. These breaches come with side effects that are often difficult to quantify, such as the loss of a company's reputation and the trust of its customers.

The prescription for these attacks has largely remained the same: identify sensitive data, build protections around where that data is stored and used, and, where possible, keep the data encrypted.

Ransomware flips the script because your data is held for ransom and the value to the attacker isn't in the data itself, but in the value you (or your organization) place on that data. That is to say, even though the data may not be sensitive in its content, it may be business critical for your organization in the short and long term.

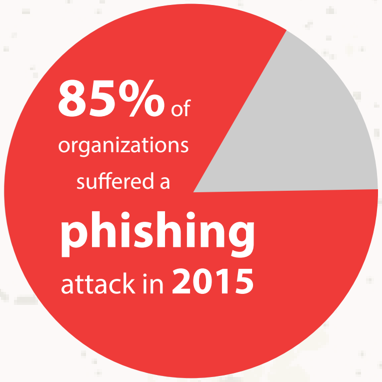
COMMODITIZATION AND RANSOMWARE-AS-A-SERVICE

The dark web is a veritable craigslist for hackers where unskilled hackers – or even your everyday civilians – can purchase the tools needed to levy advanced malware attacks. This commoditization of malware samples and tools makes it easy for attackers to get specific types of malware for targeted attacks against SMBs and distributed enterprises without spending a lot of time or energy. And because many of these businesses won't have the necessary protections in place, many will fall victim to ransomware attacks that could have otherwise been prevented.

The emergence of ransomware-as-a-service exacerbates the problem. Ransomware-as-a-service enables non-technical criminals a means to not only perpetrate these advanced malware attacks but the means to collect the profits as a service as well.

TARGETED RANSOMWARE ARRIVES

Ransomware attacks, generally facilitated by phishing emails with malicious links, typically are performed in what we call spray attacks. Hackers send emails en masse to try and infect as many people as possible. Thousands of these emails go out each day, with attackers simply playing a numbers game and hoping that someone will be naïve enough to click a link or download a file from someone they don't know. The sad reality is that many people will become infected by this method, evidenced by the fact that a reported 85% of organizations suffered a phishing attack in 2015.[3]



22%
increase in
spear-phishing
attacks from
2014-2015

Even though broad attacks remain successful, targeted spear-phishing attacks are more common than ever. Research has shown a 22% increase in spear-phishing attacks from 2014 to 2015.[3] By spending a little time researching a target, crafting a compelling email (perhaps even impersonating a coworker or friend) and designing malware, skilled attackers are able to ensure a higher degree of success in ransomware attacks. Small and midsize businesses are frequently subjected to spear-phishing campaigns, as 43% of spear-phishing attacks were aimed at businesses with 250 or fewer employees.

What's more, because these attacks are tailored to specific targets the potential for harm is even greater. A new breed of ransomware is able to seek out backups and cloud stores, making restoring your data more difficult, if not impossible. Ransomware has also evolved to extract a more calculated ransom based on the target organization and environment.

EMPLOYEES ARE THE WEAKEST LINK

Social engineering has long been used by criminals as a means of manipulating their victims. From using scare tactics like impersonating federal agencies or the police, to delivering malware via emails carefully crafted to target a specific person, social engineering is often an integral part of a ransomware attack. This places your employees on the front lines of the battle against ransomware.

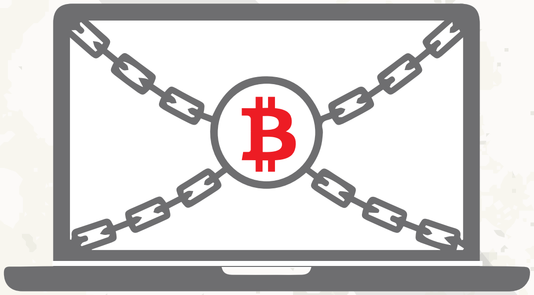
One click on a phishing email from an unsuspecting employee in accounting and your system is hacked, devices locked, business done for the day. Whether its high volume attacks, or targeted ones, it's critical that your employees are educated on what a phishing email looks like and what it is.

MITIGATING THE THREAT OF RANSOMWARE

The number of ransomware incidents has exploded in the last few years, infecting hundreds of thousands of systems worldwide. The availability of ransomware tools and the emergence of ransomware-as-a-service means attackers needn't be technically savvy. While the availability of these tools has increased the volume of ransomware attacks overall, many of these attacks can be prevented.

WatchGuard's Total Security Suite is the first UTM service available that brings enterprise-grade ransomware prevention tools to small and midsize businesses. With advanced security solutions like WebBlocker, APT Blocker and Host Ransomware Prevention, WatchGuard's Total Security Suite is any organizations best option for protecting their business from ransomware attacks.

WEBBLOCKER	WebBlocker is a fully integrated security subscription for WatchGuard appliances that allows IT administrators to manage web access and content for stronger security and control of web surfing. This module blocks malicious sites that could house ransomware, preventing successful malware downloads.
APT BLOCKER	APT Blocker is a dynamic sandboxing solution providing detailed visibility and analysis into the execution of malware. If the file has never been seen before, the files are detonated in a virtual environment to analyze the behavior and determine the threat level, protecting against advanced malware and zero-day threats.
HOST RANSOMWARE PREVENTION	Host Ransomware Prevention (HRP) detects and prevents ransomware attacks at the endpoint. HRP is built on a behavioral analytics engine that monitors a wide array of characteristics across an endpoint to determine if a given action is associated with ransomware. Once attribution is made, HRP blocks the execution before any file encryption takes place.



WatchGuard's Threat Detection and Response service provides enterprise correlation capabilities for small and midsize businesses and distributed enterprises. Don't just think there might be a problem, know if there is with industry-leading solutions that help illuminate your endpoint, detect and correlate threats, and protect your most important assets.

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-grade protection to hundreds of thousands of businesses worldwide. To learn more, visit **WatchGuard.com/TDR**.

1. https://business.kaspersky.com/cryptomalware-report-2016/5971/
2. https://business.kaspersky.com/cryptomalware-report-2016/5971/
3. https://www.wombatsecurity.com/press-releases/new-report-state-of-phishing-attacks