Healthcare Data Security:
Can You Do It on Your Own?

Ransomware has affected healthcare facilities far and wide

Digitization, big data, and mobile devices are having a revolutionary impact on modern healthcare. These innovations are easing workflow, enhancing patient care, and lowering healthcare costs, but also creating major security gaps at the same time. As healthcare practices evolve, data security often falls short of these blossoming technologies. While they enable healthcare services to leave the confines of the protected corporate network, utilizing the Internet to connect remote clinics, 3rd party laboratories, and staff while working off-site – they also increase the opportunity for hackers to break into protected systems to steal data, or even just hold it hostage in order to extort payments.

Moreover, employees are accessing the Cloud constantly. They're working all the time, from anywhere. They're using their own devices and downloading content from potentially risky sites. They're accessing Wi-Fi from environments that may – or may not – be secure. Simply put, keeping an eye on the growing multitude of security details is a daunting task. Are you up to the challenge?

What Is Layered Protection?

A layered approach to security offers easily-managed full 360° defenses, including network protection, Wi-Fi security and multi-factor authentication. Network protection starts with installing a firewall appliance , which provides out-of-the-box policies, management, and reporting tools designed for ease of deployment and ongoing management.

Unfortunately, healthcare has become a particularly popular target for ransomware extortion. Since 2017, ransomware threats have risen three-fold, with major attacks weakening health systems around the world. When a hacker took control of their network – and refused to release it without payout – Hollywood Presbyterian Medical Center paid no less than $17,000 in Bitcoin to resume normal operations. A little later, WannaCry – the now-notorious ransomware variant that leveraged a vulnerability found on older versions of Windows OS – left a multitude of infected computers in its wake: around 200,000 across 150 countries.

The healthcare sector was hit hard, causing a state of crisis in hospitals and clinics around the globe. National Health Service (NHS) facilities in England experienced computer and phone system disruption, system failures, and ultimately a wave of surgery delays, cancelled appointments, and confusion after hospital computers began displaying a ransom message demanding Bitcoin. One of the industry's largest drug manufacturers, Merck, confirmed they had also fallen prey to the forceful variant, with attacks extending throughout their global offices. Not only can these incidents have horrible short-term impact on patient outcomes, they also affect a facility's ability to compete over the long term if their reputation is tarnished.

The proliferation of these attacks proves that enterprise-grade, layered security is no longer a luxury, but rather a necessity for every organization. Brendan Patterson, VP of product management at WatchGuard Technologies, explains, "Research done by our Threat Lab shows that 38% of malware gets past legacy AV, which is why services like IPS (Intrusion Prevention Service), sandboxing, and detection and response are so critical."

Layered protection has shown in repeated tests to be the best approach to security, enabling the highest degree of coverage. Extending protection with Wi-Fi security and multi-factor authentication optimizes defenses against the multitude of attacks and allows healthcare organizations to avoid the penalties and damage arising in the aftermath of an attack.

How are cyber criminals accessing networks in the first place?

Hackers are fixating on healthcare because it's an attractive target given the distributed facilities loaded with new technology and networked devices, the large number of employees with network access and limited security knowledge, and a considerable amount of valuable data including names, email, national ID numbers, and credit card numbers. Enterprising criminals have also learned that they can exploit the time-critical need for patient data to demand payment out of healthcare facilities. The last thing any of these organizations want is for an attack to go public and drive paying patients to competing facilities for fear that their personal data will be compromised. Hackers know this too – and they're betting that they'll get a payout.

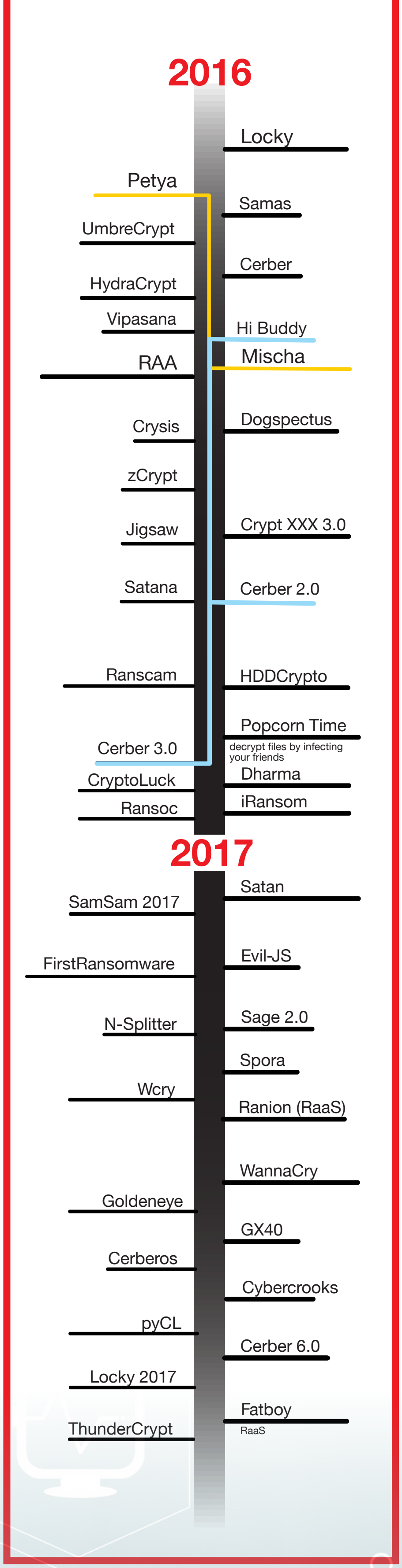
So, how do they get past existing defenses? According to Verizon's 2017/2018 data breach report, using stolen credentials is the #1 way that hackers breach networks. After all, it just takes one valid password to break in, and among all the staff, surely there's one person willing to bite on a phishing lure, or connect to a spoofed Wi-Fi access point for a man-in-the-middle attack, or share their password with other online accounts that have been breached, or use such a simple password that it can be cracked in a brute force attack. If by some chance this doesn't work, then they might throw some evasive malware they purchased from the dark web and see if your defenses aren't quite good enough to detect and prevent the attack.

MFA Is Essential Protection

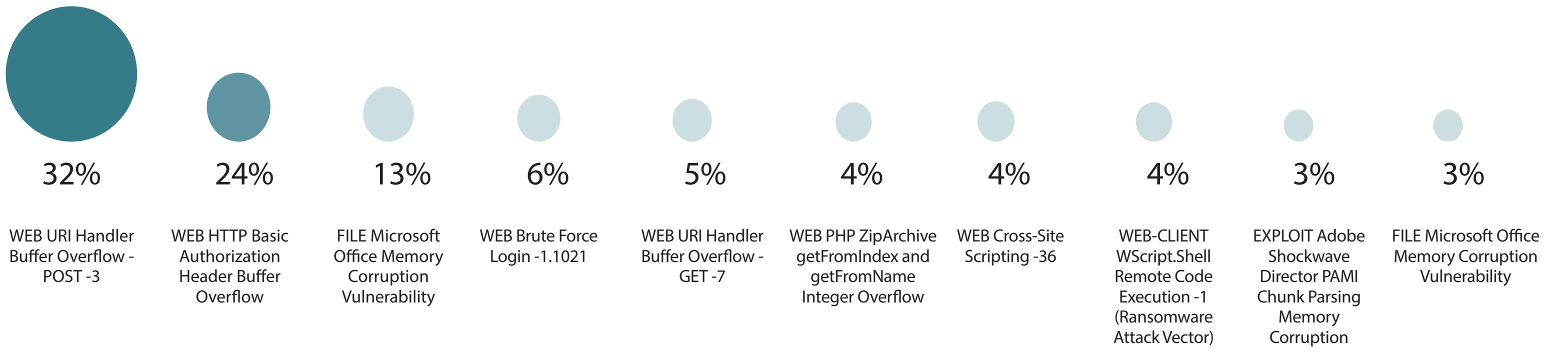
Multi-factor authentication (MFA) helps to reduce the likelihood of network disruptions and data breaches arising from lost or stolen credentials. This service can use a push message, QR code, SMS text message, or a one-time password (OTP) as an additional factor in proving the user's identity. This means that a hacker with a valid stolen password would still be denied access, protecting the networks and Cloud applications from being attacked and breached.

"Hackers can be quite innovative when they see an opportunity to make some coin," says Patterson. "Facilities need to shut down all potential points of access with advanced security that can detect evasive malware and automatically remediate it. This protection needs to be extended to the endpoints for when they leave the network." Also, a simple username and password is not enough to verify that someone requesting access to systems is truly that individual. Multi-factor authentication requires users to identify themselves with a real-time response from their phone or other device, and block a bad actor from immediately entering the network with just a valid password. Adding an overlay of Wi-Fi security that restricts users from connecting to unauthorized access points is another critical security measure to keep criminals off your networks. And with that, you have a comprehensive portfolio of security solutions to keep out
unauthorized individuals.

Ransomware Is on the Rise



Top Network Threats Seen During Q2 2018



Name	Threat Category	Affected Products	CVE Number	Count
WEB URI Handler Buffer Overflow - POST -3	Web Client	ALL	CVE-2011-1965	CVE-2011-1965
WEB HTTP Basic Authorization Header Buffer Overflow	Web Server	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	CVE-2009-0183	CVE-2009-0183
FILE Microsoft Office Memory Corruption Vulnerability	Office Document	Windows	CVE-2016-7231	CVE-2016-7231
WEB Brute Force Login -1.1021	Web Server	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	N/A	N/A
WEB URI Handler Buffer Overflow - GET -7	Web Server	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	NA	NA
WEB PHP ZipArchive getFromIndex and getFromName Integer Overflow	Web Server	Windows, Linux, FreeBSD, Other Unix	CVE-2016-3078	CVE-2016-3078
WEB Cross-Site Scripting -36	Web Client	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	CVE-2011-2133	CVE-2011-2133
WEB-CLIENT WScript.Shell Remote Code Execution -1 (Ransomware Attack Vector)	Web Client	Windows	CVE-2006-4704	CVE-2006-4704
EXPLOIT Adobe Shockwave Director PAMI Chunk Parsing Memory Corruption	Web Client	Windows	CVE-2010-2872	CVE-2010-2872
FILE Microsoft Office Memory Corruption Vulnerability	Web Server	Nginx	CVE-2016-3316	CVE-2016-3316

Healthcare Organizations Benefit the Most from Outsourced Expertise

In this new era of computing, continuous monitoring, testing, and updating across your entire network security infrastructure are key to providing effective protection. Threats are constantly evolving – your defenses should too, and security expertise is essential for staying ahead of threats. A solution provider can help you stay up to date on complex security environments and can help simplify security solutions.

More than ever, healthcare organizations are engaging with Managed Security Service Providers (MSSPs) and relying on their security expertise to increase their security measures now and in the future. Brent Morris of Success Computer Consulting remarks, “Digital healthcare environments are complex, but security doesn’t have to be. We run a Security Operations Center that constantly assesses our clients’ changing digital environment and we provide a fresh set of eyes to advise on potential gaps in security.” Best yet, MSSP partners perform security-related activities for their customers using layered security, which include firewalling and security services, as well as the management and visibility needed to keep cyber criminals at bay. “Our experts stay on top of the security landscape and implement the technologies needed to protect our clients,” says Morris, “we are successful when IT staff at managed sites are free to focus on the critical needs associated with delivering excellent healthcare… knowing that we’ve got their security needs covered.”

MSSPs can also help to educate workers using both training and technologies to modify "happy clicker" behavior – where a click on the wrong link at the right time results in a successful phishing attack. Morris emphasizes, "Because an effective awareness program requires a professional approach with an expert, healthcare facilities benefit from outsourced training provided by specialists. Even more effective is to add technologies that identify a potential phishing attempt and provide education at the moment the riskly click occurred. That's behavior modification that never fades."

Wi-Fi MitM Attack

It's more common than you realize. With 60% of all Internet connections occurring over Wi-Fi, it's safe to say that Wi-Fi access has become an everyday essential for the vast majority. Yet, man-in-the-middle Wi-Fi attacks have created major damage in recent years. This attack is simple, and silent. The unwitting user attempts to connect to a Wi-Fi hotspot, but instead connects to an alternate access point with the same SSID. The hacker is happy to let the user through to the Internet, but is watching everything they do, hoping to lift passwords, credit card numbers and other valuable data.

In the end, security needs have gone beyond what individual healthcare organizations can provide on their own. They need a team approach to keep the company, employees and patients safe from attacks. "It's the combination of the right layered defenses, the right network security provider and the right MSSP that keeps some healthcare organizations protected while others are consistently targeted," says Patterson. "While NHS in the UK was suffering the effects of the WannaCry attack, Care Plus Group, also in the UK, was unaffected. Why? They had the right team working with them, including layered defense in-depth with WatchGuard and a strong IT services partner in F4IT. It saved them from suffering the many expenses and headaches associated with a major breach."

MSSP Services

- Intrusion prevention systems (IPS)
- Web content filtering
- Antivirus (AV), Anti-spam
- Firewalls (UTMs, NGFWs)
- VPN
- Vulnerability scanning
- Patch management
- Data loss prevention (DLP)
- Threat intelligence
- Identity access management (IAM)
- Privileged access management (PAM)
- Risk assessments and gap analysis
- Policy development and risk management
- Solution scoping
- Solution/tool research and requisition
- Solution implementation
- Management of security systems
- Configuration management
- Security updates
- Reporting, auditing, and compliance
- Training and education

RESOURCES:

- ISR report:
watchguard.com/wgrd-resource-center/security-report
- F4IT Case Study:
watchguard.com/wgrd-resource-center/case-study/f4-it
- Wi-Fi MitM video:
watchguard.com/wgrd-resource-center/webinars/secure-wi-fi-webinars

CITATIONS:

- Verizon security report

WatchGuard®

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. Part No. WGCE671386_121818