ExtraHop

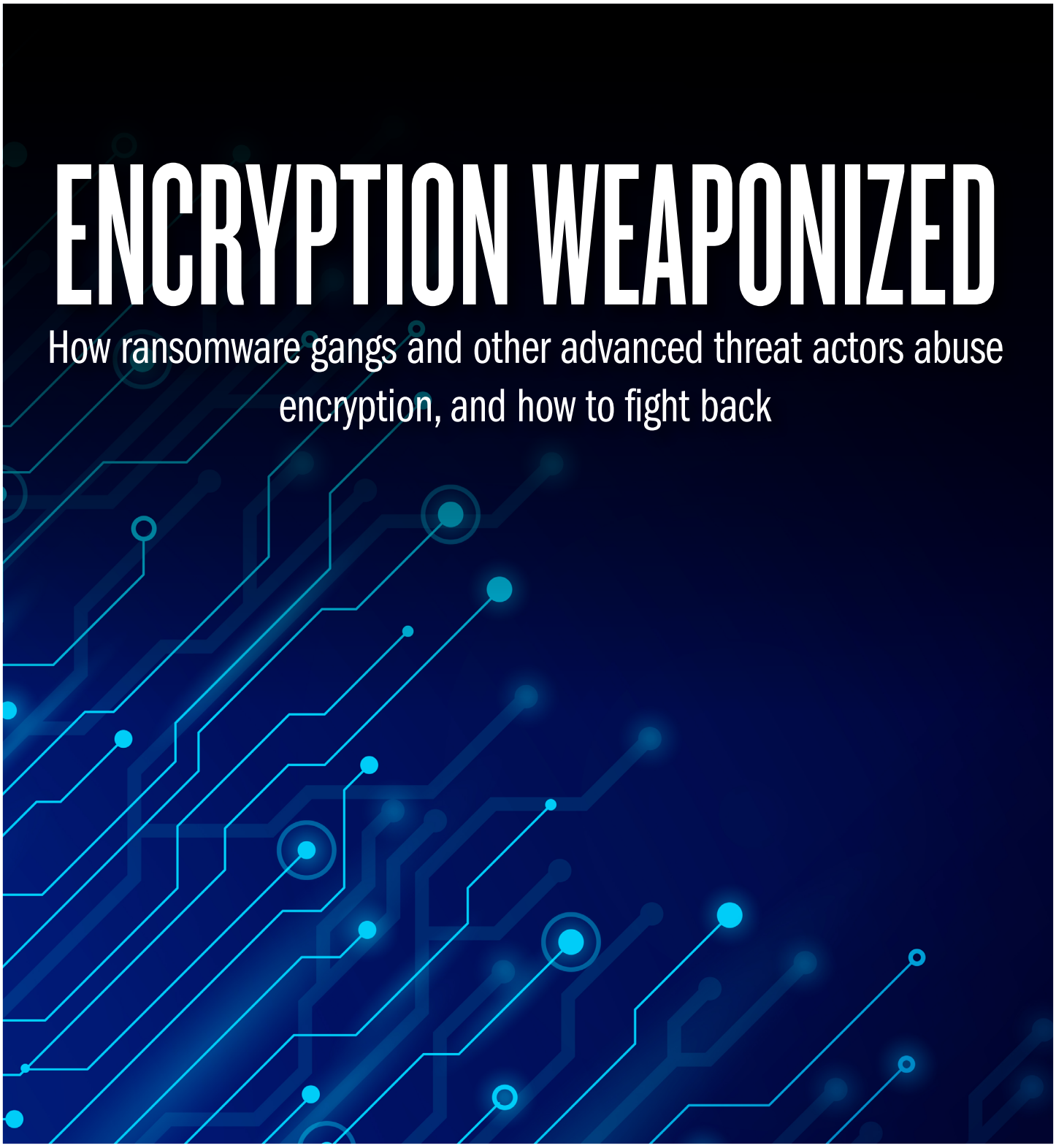
ExpertFocus

March 2022

Brought to you by ExtraHop

ENCRYPTION WEAPONIZED

How ransomware gangs and other advanced threat actors abuse encryption, and how to fight back



Decryption matters

Ransomware gangs actively turn encryption against enterprises. George V. Hulme talks to security experts from ExtraHop and elsewhere on how to turn the tide.

For each step enterprises take to protect themselves from ransomware, criminal cyber gangs manage to place another landmine at their feet.

Ransomware gangs make every move they can to gain an edge, from utilizing widespread software vulnerabilities, common configuration errors and zero-day vulnerabilities to tricking end-users at a careless moment.

Increasingly, as you'll see in this report, they are turning capabilities typically used to protect enterprises into attack tools — the very encryption organizations use to protect their traffic, systems, and data.

Richard W. Downing, deputy assistant attorney general in the criminal division of the U.S. Department of Justice, recently told the U.S. Senate hearing on ransomware that it's a serious threat to public safety and national and economic security. Ransomware has been used to attack municipal governments, police departments, and critical infrastructure such as suppliers of food and gasoline. Some specifically targeted health care facilities during the pandemic, taking advantage of the global crisis to extort victims who are especially vulnerable and cannot afford to lose access to data.

A shift in strategy and tactics

The business model for ransomware has evolved as well. Cybercriminals are actively increasing their reach through ransomware-as-a-service — an underground business that sells ransomware to anybody. In other words, they're giving would-be cyber criminals the ability to encrypt people's data and hold it for ransom. While the RaaS provider may not conduct the attacks, they control it behind the scenes.

Ransomware gangs have changed their tactics in other ways. In prior years, attackers would gain access to a network, encrypt what they could, and then demand payment. Currently, attackers are undertaking so-called double extortion attacks. In these attacks, they will first steal the data by making copies. Then they will encrypt the enterprise data before demanding their extortion payment. Now, should an enterprise refuse to pay the ransom in order to get the decryption keys, attackers threaten to release the data on the open Internet or dark web.

"This has come about because people have grown better at backing up and taking other security measures," says Jamie Moles, senior technical marketing manager at ExtraHop. "People have put plans in place to deal with the standard ransomware attack. That, combined with the rising cost of Bitcoin has made paying out a bad business plan."

Turning encryption against defenders

In a recent CyberRisk Alliance survey, State of Ransomware: Invest now or pay later, 43% of respondents reported having endured at least one ransomware attack within the past two years. Of those, 58% paid a ransom, 29% found the data stolen from them on the dark web, and 44% lost additional revenue due to the attack.

Also, 37% of respondents said they lack an adequate security budget, while 32% believe they're powerless to prevent ransomware attacks because threat actors are too well-funded and sophisticated. Many respondents lack strong confidence in their ability to fight ransomware. "New emerging cyber-attacks are penetrating the most secure methods of protection," said one executive.

The experts we interviewed for this report agreed. CISOs are very concerned that attackers will find

> “Attackers use encryption to protect communications between the target and their command-and-control servers to evade leaving identifiable indications of compromise, and to deliver malicious payloads while evading detection.”
>
> *– Benny Czarny, founder and CEO at OPSWAT.*

new ways to conduct their attacks regardless of the defenses they put into place.

“Organizations fear new strains of ransomware for which there are no signatures. That means their intrusion detection systems miss it. That means security systems scanning email for binary signatures also miss it,” explains Moles.

One increasingly popular technique among ransomware attackers is to hide within the encryption enterprises have deployed at the perimeter as well as inside hybrid and cloud networks to protect their systems and data.

This way, they can hide how they attempt to move laterally through the organization, their command-control activities, their data exfiltration, and more.

In July 2021, the U.S. Cybersecurity and Infrastructure Security Agency, the Australian Cyber Security Center, the United Kingdom’s National Cyber Security Center, and the U.S. Federal Bureau of Investigation found that encrypted protocols such as Microsoft Server Message Block v3 are used to mask lateral movement and other advanced tactics in 60% of the 30 most exploited network vulnerabilities.

“Attackers use encryption to protect communications between the target and their command-and-control servers to evade leaving identifiable indications of compromise, and to deliver malicious payloads while evading detection. For example, a common technique to evade malware detection is to encrypt the payload or encrypt content in the payload,” says Benny Czarny, founder and CEO at OPSWAT.

Camila Serrano, CSO at MediaPeanut, says she’s witnessed numerous cases of malware hidden within encryption.

“I have observed that malware was snuck into organizations under the guise of encryption in roughly half of the cyber assaults,” Serrano says. “Data encryption has been known to mask malware in over half of cyber intrusions last year simply because SSL encryption prevents many security technologies from detecting the infection, which poses a big challenge to the cybersecurity community.”

Encrypted protocols used in attacks

Jeff Costlow, Deputy CISO at ExtraHop, says encrypted traffic has been exploited in some of the most significant cyberattacks and attack techniques within the past year, from Sunburst and Kaseya to PrintNightmare and ProxyLogon.

Attackers use numerous encryption protocols to hide within networks. Consider Microsoft Server Message Block v3 (SMBv3). SMBv3 is used within most Microsoft networks and has been the default installed with Microsoft servers for years. Microsoft Server Message Block is a fundamental communication protocol for Microsoft networks and provides shared access to related files and printers.

While the first version of SMB was released in 1996, it wasn’t until SMB v3.0.2 arrived with Windows 8 and Windows Server 2012 that

"I have observed that malware was snuck into organizations under the guise of encryption in roughly half of the cyber assaults. Data encryption has been known to mask malware in over half of cyber intrusions last year simply because SSL encryption prevents many security technologies from detecting the infection, which poses a big challenge to the cybersecurity community."

– Camila Serrano, CSO at MediaPeanut

end-to-end encryption arrived. That version also included an AES signing algorithm. And with Windows 10 and Windows Server 2016, SMB 3.1.1 further enhanced its encryption capabilities.

"Encryption has to be turned on, especially on file shares. But if you have SMB-encrypted traffic on your network, while it protects you, you also can't see a lot of the lateral movement performed by threat actors," says Moles.

Other Microsoft protocols particularly matter in lateral attacker movement, explains Moles. These include Windows Management Instrumentation (WMI), Secure RPC (Remote Procedure Call), and Windows Remote Management.

Common utilities, such as those that come with Microsoft Sysinternals Suite, are also vulnerable to attackers turning the encryption against the organization. These include PsExec, the light telnet-replacement application. PsExec enables admins and others to execute software on other systems. With version 2.1, encryption was added with PsExec. And with this enhancement, all communications between the local and remote system are encrypted.

"PsExec uses Microsoft protocol-level encryption to encrypt the commands it's sending across the network," explains Moles. "If an attacker uses that feature, perhaps to launch a remote service on another machine, the victim organization is not going to see what is happening," he explains.

When attackers combine encryption with other techniques to lower their visibility, they become even more clandestine. Consider traditional reconnaissance techniques, such as scanning network addresses or brute force attacks, and how they can create noise on the network. These techniques will often trigger intrusion detection/prevention systems and be more readily spotted by threat hunters.

"What we've seen nowadays is a move away from scanning. Nowadays, instead of trying to find domain controllers, and other network equipment, with scanning and ICMP (Internet Control Message Protocol) pings to try and map target networks, they're being much more careful," explains Moles.

This means attackers hiding within encrypted communications may choose to look at route tables on the local network and search the lower or higher range of the subnet. "When IT builds servers, they often put them either at the low or the high range subnet," says Moles.

The importance of decryption

There are a number of different approaches to detecting malicious activity hidden within encrypted

"The idea behind encrypted traffic analysis is that, although you can't see the content of the traffic, you can conduct metadata analysis. When you compare metadata with known normal traffic and combine that with threat intel, you can gather some actionable information if you have enough data. However, it still leaves gaps."

– Jamie Moles, senior technical marketing manager at ExtraHop

network traffic. Historically, decryption has largely been performed at the firewall with an emphasis on decrypting north-south traffic. While this is still important, it's not sufficient. Many attack tactics now leverage encryption inside the perimeter, including Activity Directory and other Microsoft protocols.

When it comes to detecting malicious activity in encrypted east-west traffic, there are two primary approaches. The more common approach is encrypted traffic analysis (ETA), which originally came into existence to evaluate perimeter-based encryption protocols such as HTTPS, FTPs, SSL and TLSs.

"The idea behind encrypted traffic analysis is that, although you can't see the content of the traffic, you can conduct metadata analysis," Moles says. "When you compare metadata with known normal traffic and combine that with threat intel, you can gather some actionable information if you have enough data. However, it still leaves gaps."

Consider a standard web (HTTP) transaction. During a demonstration, an ExtraHop expert detailed several attacks leveraging encryption.

- One example involves the injection of malicious code. ETA can help determine who sent a particular request, who received it, the time it occurred, as well as a rough idea of the size of the transaction. However, without decryption, it is impossible to tell whether that activity is a cross-site scripting attack or a legitimate server request since it's encrypted. Another example involved a web directory scan. ETA showed the time and size of the transaction, as well as both the sender and recipient. Without fully decrypting this traffic, however, the security analyst couldn't determine if the attackers were building intelligence on the systems and preparing themselves for a successful attack.
- Another example involved a web directory scan. ETA showed the time and size of the transaction, as well as both the sender and recipient. Without fully decrypting this traffic, however, the security analyst couldn't determine if the attackers were building intelligence on the systems and preparing themselves for a successful attack.
- The final example involved data exfiltration. ETA showed that the request was coming from a trusted requester, as well as the time and the rough size of the request. But ETA cannot detect that the requester was compromised, and the attacker was using their credentials to exfiltrate a sizable amount of data. While large transactions may be flagged without decrypting them, the alarm

“If you can’t inspect it, by default, it should be dropped and not allowed to pass either in or out of your system.”

– Keatron Evans, principal security researcher, instructor, and author at Infosec Institute

would be triggered much more rapidly had the traffic and nature of the transaction been visible.

Decrypting network traffic enables security teams to dig deep into elements of transactions and see exactly what is happening on the network.

Keatron Evans, principal security researcher, instructor, and author at Infosec Institute, says organizations need to make sure that they can inspect as much traffic as they can.

“If you can’t inspect it, by default, it should be dropped and not allowed to pass either in or out of your system,” Evans says. “While this is a best-case scenario, it is usually not followed 100% of the time, except in some rare high-security situations.” Still, the goal is to get as close to full-compliance as possible as you build out solutions.

Others essentially agree. “The ability to decrypt network traffic is extremely important as a means of detecting anomalous and malicious behavior within an organization’s IT network,” says Tony Cook, head of threat intelligence, DFIR, at GuidePoint Security. “Without the ability to decrypt network traffic, it becomes difficult to identify bad or risky network behavior within the network. Organizations should place importance on decrypting network traffic where possible and balance that with any regulatory or ethical obligations regarding privacy,” Cook says.

While ETA provides the ability to study an encrypted traffic stream and analyze the attributes of that stream, security tools have come to market that can decrypt and fully parse Microsoft Active Directory authentication protocols (Kerberos and NTLM) and Microsoft Windows application-level protocols using passive, out-of-band decryption for rapid and accurate detection of advanced threat activity.

And some tools can decrypt and evaluate the SSL traffic and the TLS 1.1 and 1.2 traffic, as long as the organization owns the public key infrastructure. At the same time, other solutions will forward the ephemeral keys for individual sessions within TLS 1.3.

This provides the ability to spot malicious behavior with greater certainty more readily.

“Decryption has numerous benefits. First, decryption detects malicious activity earlier in an attack campaign. Second, decryption improves mean time to response because it provides valuable context to ensure rapid detection, scoping, investigation, and remediation of threats. And finally, decryption allows a full forensic record for post-compromise investigations,” Costlow says.

As ransomware gangs and other threat actors continue to weaponize encryption, security teams will need every edge they can find. ■

ExpertFocus

Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

Learn more at [www.extrahop.com.](http://www.extrahop.com)


“Well, the basic idea is I break into a company’s network, encrypt their files and hold the keys for ransom.”
Meet Ransomware
www.extrahop.com/meet-ransomware
ExtraHop