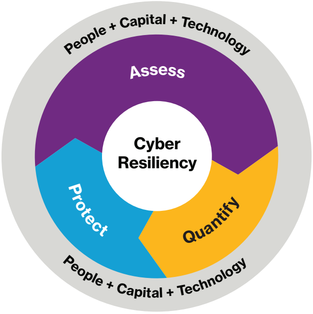


Decode threat.

Cryptojacking: Ransomware’s sneaky cousin is the new kid on the cyber block

By Dan Twersky, Willis Towers Watson

*Past editions of **Decode Cyber Brief** have focused on the threat of ransomware and the substantial cyber risk it brings – namely that of network business interruption for industries that historically had little to no risk for lack of records in possession. Fewer records means less of a chance of notification obligations and/or legal liability. Now, even these industries are no longer “cyber proof”, rather, they too can be subjected to losses totaling hundreds of millions of dollars resulting from network business interruption.*

A marked shift by cyber criminals from the traditional theft of Personally Identifiable Information (PII) and credit card data to ransomware has already occurred. Ransomware attacks are deemed to be far more safe and efficient (for the hacker) compared to perpetuating an elaborate hack of an organization’s network, for the following reasons:

- It can be bought off the shelf via the “dark web” and deployed simultaneously to hundreds of targets.
- It requires minimal communication with the victim, who, after paying the ransom is the party tasked with implementing the decryption process.
- It has a far shorter timeline to an eventual payday, one which results in highly untraceable and valuable digital currency.

Given the ease of ransomware, these types of attacks have grown in size and severity and show no sign of letting up. However, a variant of the ransomware scheme known as “cryptojacking” has become prolific over the past year, and according to some security experts, has even superseded ransomware as the top malware threat.

Welcome to cryptojacking

Cryptocurrency is typically purchased through an online exchange. However, it can also be obtained through a process called “mining”, by which complex equations are solved by powerful computers in order to verify transactions and/or cause new currency to be released and earned. The necessary hardware and the resources needed to power that machinery can be quite expensive.

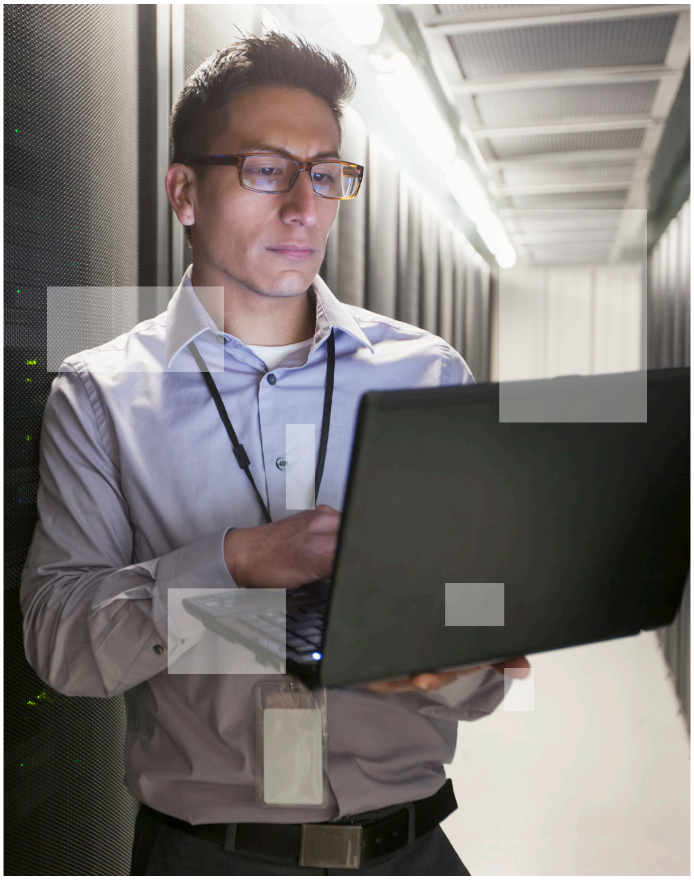
Not wanting to miss out on this potentially lucrative opportunity, but also in search of a scheme that would draw less attention from victims and, in turn, law enforcement agencies, cyber criminals have developed malware that mines cryptocurrency using the hardware and resources of unsuspecting third parties. The malware is generally written to “mine” during the middle of the night to help avoid detection, and purposely at a time when the equipment and bandwidth of the third party is not otherwise in use, thereby maximizing its utility.

Another advantage for cyber criminals is that the malware can be spread to countless machines, compounding the mining activity, whereas with ransomware, income is only derived from those victims who actually pay up.

Beware of cryptojacking schemes

Cryptojacking malware is generally transmitted in three ways:

1. **Through phishing,** in which individuals are sent emails with attachments or links masked as legitimate, but in reality contain or lead to the malware, which is then secretly uploaded onto the person's computer system.
2. **Through the insertion of scripts into ads on websites.** Through this method, the malware is never installed on the computer system, but executed through the web browser where it directs the infected machine to perform mining activities for the benefit of the cyber criminal.
3. **Via Internet of Things ("IoT") connectivity,** although it remains unclear how worthwhile the hijacking of IoT devices can be for this purpose. Despite often lacking sufficient security controls, IoT devices possess far less computing power than an actual computer. There are reports, however, of botnets previously commanded to send spam messages or perform Distributed Denial of Service ("DDoS") attacks now being retooled to mine for cryptocurrency.



The price of cryptojacking

Instances of cryptojacking have increased exponentially in 2017[1], and by 459 percent through the fall of 2018.[2] But can cryptojacking essentially be viewed as a victimless crime? Far from it. The damages to a victim can vary, but are likely to include one or more of the following:

- Overruns of bandwidth allowances, resulting in additional costs (e.g., power and electricity) or "throttling" (deliberate regulation of the rate of data transfer) by internet service providers,
- The risk of property damage to hardware due to overheating and other mechanical breakdown or destruction, as well as loss of locally-stored data should the hardware fail,
- Business interruption due to hardware failure and data loss, but also due to a slowdown in the ability to conduct business due to the tie-up of critical resources from mining activities, and
- Increased security risk, as security experts have advised that in the cyber criminals' efforts to make their malware more productive, they can also disable additional security productions, open ports, and install additional malware that will carry out a different attack on the network at a later time.

Guarding against a cryptojacking event

Given the very real and tangible risk to organizations, taking precautions against cryptojacking is vital:

- **For phishing risk:** Perpetually remind employees to think critically about their cyber activities through regular training and testing (including mock phishing campaigns). Measure employee awareness and understanding of the risks through engagement surveys.
- **For website ad risk:** Here, technology solutions generally work best. While employees can be counseled to avoid non-essential or lesser-known websites, cryptomining script can run undetected to even the (cyber) savviest of employees. For example, a script was recently detected running in the background of a popular media company's online streaming website and earlier this year, cryptomining code was found on a leading newspaper's website. Therefore, technology remains a key component of defense. In fact, these examples serve as a good reminder that technology, as well as people solutions, should both be implemented in tandem in order to best mitigate the chance of an attack.

[1] Semantec Internet Security Threat Report-Volume 23, March 2018
[2] "The Illicit Cryptocurrency Mining Threat," https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf

Cyberinsurance for cryptojacking

Cyberinsurance can also help companies reduce the impact of losses due to cryptojacking. The detection of cryptojacking malware will generally trigger the cyber incident response coverage under a cyber policy, providing coverage for legal and forensics work at a minimum. To the extent the malware has resulted in a demonstrable interruption in the operation of the business, and loss of income could be substantiated, cyberinsurance policies (and certain property policies) could also provide coverage under the business interruption insuring agreement as extra expenses incurred.

In instances where the malware results in damage to physical hardware, coverage may be available under a property insurance policy. For damage to electronic data, subject to the language of the particular cyber policy, coverage may be available for the cost of restoring the data, while some property insurance policies may provide coverage for the lost value of that data if it cannot be restored.

It remains to be seen whether the steep decline in cryptocurrency values over the past year will serve to dissuade cyber criminals from carrying out these attacks and encourage them to move on to other schemes. In the meantime, the cryptojacking threat is real and should be treated as more than a simple nuisance. A holistic, three-pronged approach involving technology, risk transfer, and people-based solutions remains the optimal strategy.

Contact

Dan Twersky
+1 212 915 8580
dan.twersky@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-NA-2018-WTW163861