2018. www.zdnet.com/article/gates-the-password-is-dead/.

5. 'Lenovo, Nok Nok Labs, PayPal, and Validity Lead an Open Industry Alliance to Revolutionize Online Authentication'. FIDO Alliance, press release, 12 Feb 2013. Accessed Jun 2018. https://fidoalliance.org/lenovo-nok-nok-labs-paypal-and-validity-lead-an-open-industry-alliance-to-revolutionize-online-authentication.
6. 'FIDO Alliance and W3C Achieve Major Standards Milestone in Global Effort Towards Simpler, Stronger Authentication on the Web'. FIDO, press release, 10 Apr 2018. Accessed Jun 2018. https://fidoalliance.org/fido-alliance-and-w3c-achieve-major-standards-milestone-in-global-effort-towards-simpler-stronger-authentication-on-the-web/.
7. Furnell, S. 'An assessment of website password practices'. Computers & Security, vol.26, nos.7-8, 2007, pp.445-451. Accessed Jun 2018. www.sciencedirect.com/science/article/pii/S0167404807001083.
8. Furnell, S. 'Assessing password guidance and enforcement on leading websites'. Computer Fraud & Security, Dec 2011, pp.10-18. Accessed Jun 2018. www.sciencedirect.com/science/article/pii/S1361372311701233.
9. Furnell, S. 'Password practices on leading websites – revisited'. Computer Fraud & Security, Dec 2014, pp.5-11. Accessed Jun 2018. www.sciencedirect.com/science/article/pii/S136137231470555X.
10. 'About account security'. Twitter Help Centre. Accessed Jun 2018. https://help.twitter.com/en/safety-and-security/account-security-tips.
11. Komanduri, S; Shay, R; Kelley, PG; Mazurek, ML; Bauer, L; Christin, N; Cranor, LF; Serge, E. 'Of passwords and people: measuring the effect of password-composition policies'. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems'. 7-12 May 2011, Vancouver, BC, Canada.
12. 'Worst Passwords of 2017 – Top 100'. SplashData. Accessed Jun 2018. www.teamsid.com/worst-passwords-2017-full-list/.
13. Ur, B; Kelley, PG; Komanduri, S; Lee, J; Maass, M; Mazurek, ML; Passaro, T; Shay, R; Vidas, T; Bauer, L; Christin, N; Cranor, LF. 'How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation'. Proceedings of the 21st USENIX conference on Security symposium, USENIX Association Berkeley, CA, 8-10 Aug 2012.
14. Thomson, I. 'Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication'. The Register, 17 Jan 2018. Accessed Jun 2018. www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/.
15. Furnell, S; Khern-am-nuai, W; Esmael, R; Yang, W; Li, N. 'Enhancing security behaviour by supporting the user'. Computers & Security, Vol.75, pp.1-9, 2018. Accessed Jun 2018. www.sciencedirect.com/science/article/pii/S0167404818300385.
16. Shay, R; Komanduri, S; Durity, AL; Huh, P; Mazurek, ML; Segreti, SM; Ur, B; Bauer, L; Christin, N; Cranor, LF. 'Designing Password Policies for Strength and Usability'. ACM Transactions on Information and Systems Security, Vol.18 Issue 4, May 2016.

The role of crypto-currency in cybercrime

Aaron Higbee, Cofense

Aaron Higbee

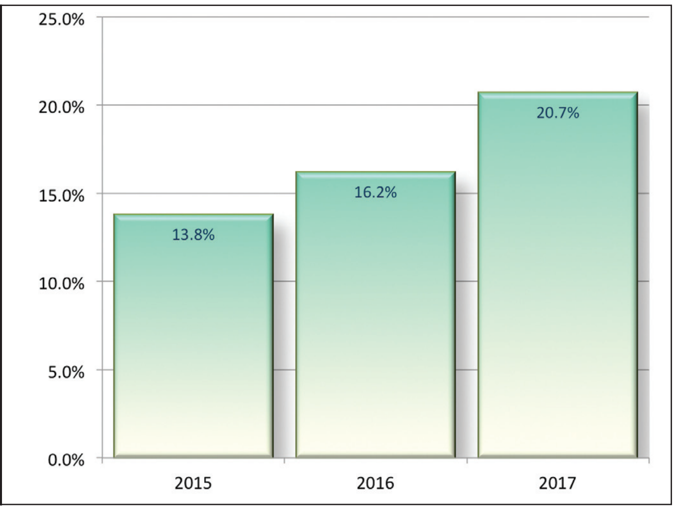
The first crypto-currency appeared in 2009 when Bitcoin was born. Since then, numerous others have entered the market. The market for crypto-currencies has been incredibly volatile and, at its peak in 2017, one bitcoin was worth over $11,200, although it is now suffering from sustained losses in 2018.[1,2] These peaks and troughs have made crypto-currency value a popular media topic and hackers too have taken notice.

For example: hackers take control of a victim's devices to mine digital currency, ransomware attacks now demand payment in crypto-currency, and the topic of crypto-currency can be used in a phishing attack. Undoubtedly, crypto-currency is transforming cybercrime. It's a method of making money, a preferred payment option and, in some cases, a lure for phishing scams.

Mining applications

Crypto-currencies log the history of transactions on a distributed ledger. This process is called mining and requires masses of computing power. In return, miners are paid in crypto-currency. To generate this sort of computer power, hackers are looking to botnets – a network of infected computers under a hacker's control – to log transactions and 'mine'.

The ability to command machines for mining is achieved through phishing emails sharing a compromised link



Reporting rates for phishing attempts have risen over the past few years, reducing organisations' susceptibility to these attacks. Source: Cofense.

that directs users to a website domain that allows hackers to run a short script designed to begin the mining. The Monera crypto-currency has been the most popular currency associated with this type of hack, as it uses calculations that can run on normal computing devices, rather than the specialised applications that are used for other crypto-currencies such as Bitcoin.

Hackers have also added mining plugins to websites to take control of people's devices and mine valuable crypto-currencies. Coinhive, for example, is a popular mining application which many hackers have been able to install on victims' devices without permission, using up their battery and compute power. What's more, this hack is not limited to laptops or computers; hackers are increasingly targeting victims' mobile phones. For instance, Android apps available on Google Play were found encoded with malicious mining capabilities. In these cases, the JavaScript runs code making this process invisible to the user. While mobile phone hacks generate much less profit compared to computer devices, both type of device are vulnerable to hacking.

There has been some effort to protect against mining malware. Google added specific protections in its web browser, Google Chrome, while anti-virus firms have updated software to detect and disable unauthorised mining applications. The main mining application, Coinhive, has also put measures in place to ask users for their permission to mine, protecting against hackers.

Ransomware payments

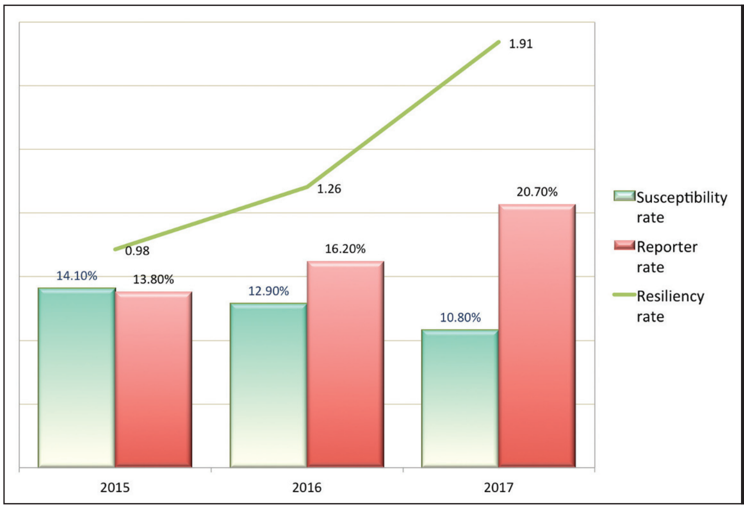
Last year, 54% of UK companies experienced ransomware attacks.[3] These often begin with a phishing attack that convinces a user to open a compromised email and click on a malicious link, granting the hacker access to the network. Once inside the network, the attackers can siphon information, encrypt it and demand a ransom for its decryption. In some cases, the ransom is demanded in crypto-currency.

Last year's WannaCry attack was the largest ransomware attack in history, affecting Windows systems all over the world, including many used by the NHS. The hackers behind the NHS attack demanded ransom payments in the form of bitcoins. Since then, other ransomware attacks have demanded ransom to be paid in crypto-currencies and some hackers have offered victims the choice to negotiate the ransom value.

Where hackers once demanded payments via Western Union or PayPal, crypto-currencies have transformed the field. One likely reason for this shift is the anonymity of using crypto-currency; payments are untraceable as they do not link back to bank accounts or addresses. This allows hackers to cover up their steps, making it easier for them to repeatedly get away with these types of attacks. To collect the ransoms paid in crypto-currency, some hackers have gone as far as to create a QR code that contains a Bitcoin wallet address. The Sage ransomware attack, which occurred in 2017, used this technique, presenting an interactive ransom note to victims with a QR code. After several collections from separate wallets, hackers can transfer all their crypto-currencies into one large wallet and reap their reward.

People now debate whether untraceable crypto-currency is causing ransomware attacks to increase. Other security breaches such as trojans, where bank details are stolen, are more traceable due to the evidence in the transaction history. Therefore, such attacks hold more risk.

However, the future of using crypto-currency in ransoms isn't certain. For example, as the value continues to fluctuate, it will be difficult for hackers to know the amount they are demanding from victims. Potentially, values will vary too much to make it worth hackers' while, or be so unfeasible in price that ransoms wouldn't be paid. This is perhaps why the Scarab ransomware allowed victims to negotiate the amount of bitcoin they



Reporting rates have increased while susceptibility rates have decreased, leading to greater resiliency. Source: Cofense.

paid. The change in Bitcoin's market price is also changing the debate around the crypto-currency's role in cybercrime, which could leave a space for other digital currencies to fill.

Phishing lures

There is a number of reasons why a hacker would launch a phishing attack, from siphoning off information, turning a victim's computer into part of a botnet, or using it as an access point to dwell within a network. The most effective way of getting victims to click is through an email that is targeted or topical. In the world of crypto-currency, imagine an email discussing Bitcoin's fluctuating value. Internet users trading Bitcoin might be intrigued enough to open the email and click on the link. This would enable the hacker to penetrate the network.

More recently, new outlets have reported on a particular Monero mining software that runs in a browser. The site most commonly associated with this behaviour is the aforementioned Coinhive. The level of exploitation is such that recently CheckPoint Software said that Coinhive miners were their 'most wanted' malware, with some 55% of their customers exposed to one or more crypto-currency mining malware families.

We know from experience that many email recipients, even if they believe an email is likely to be a phish, will still click on it simply because they are curious. Many believe that if it is a phish, they will be smart enough to recognise it once they see the page and 'not fall for it'.

The trend now is to embed the miner into more traditional credential-phishing sites, where an email lures you to a fake website designed to steal the user ID and password to an online service, email system or financial institution. When this approach is used, popular browsers launch instances of themselves which are hidden from the user, allowing coin-mining to continue in the background, even if the user has closed all the browser windows he or she can see.

An evaluation of dozens of phishing sites that launch 'in the browser' crypto-miners, including those that phishers place on already compromised servers, has so far found that they have all been linked to Coinhive. While there may be legitimate reasons why a company might want its idle machines to mine for Monero, surely most businesses would rather not have their machines used to enrich strangers.

A simple fix is to block all access to 'coin-hive.com' or 'coinhive.com' from your network – access that shouldn't be needed for employees' day-to-day work. Be aware that if these URLs are blocked, some JavaScript will load the session from an alternatively named domain. Network administrators might consider observing traffic immediately after rejecting traffic to Coinhive, just to be extra cautious. There are other browser-based mining scripts, but Coinhive is the site most actively exploited. Many anti-virus products also provide protection from this class of 'probably unwanted programs' and there are even browser plugins, such as 'No Coin', that claim to offer protection.

Building resiliency

While the crypto-currency market can be unpredictable, as long as there is money to be made, hackers will be after it. Building resiliency to any attack often comes down to protecting against phishing emails. If people can spot a suspicious email, they can stop hackers in their tracks.

With phishing attacks up 65% worldwide, a strong defence is critical.[4] Businesses are in a perfect position to help employees spot phishing attacks seeking to deliver ransomware. Phishing simulations are the most successful way to do this. They condition users to recognise and report fraudulent emails and the more users report suspicious emails, the less susceptible they become to attacks. In 2017, reporting rates were up more than 4% annually, with susceptibility rates dropping 2%.

It is also important to educate users to the phishing emails making the rounds. If they're given the most up-to-date intelligence on what to look for, employees can help IT teams catch malicious emails. IT, in turn, can more effectively respond to security threats and expel hackers from the network if employees supply real-time intelligence.

Remember, even when facing newer threats fuelled by crypto-currency, it takes more than technology to defeat the hackers. You need vigilant humans, too.

About the author

Aaron Higbee is the co-founder and CTO of Cofense (formerly PhishMe), directing all aspects of development and research that drives the feature set of this solution. The Cofense method for awareness training was incubated from consulting services provided by Intrepidus Group, a company that Higbee co-founded with Rohyt Belani in 2007.

References

1. Desai, Neera. 'Locky-Like Campaign Demonstrates Recent Evolving Trends in Ransomware'. Cofense, 7 Dec 2017. Accessed May 2018. https://cofense.com/locky-like-campaign-demonstrates-recent-evolving-trends-ransomware/.
2. Bovaird, Charles. 'Crypto market down nearly 40% from all-time high'. Forbes, 14 Sep 2017. Accessed May 2018. www.forbes.com/sites/cbovaird/2017/09/14/crypto-market-down-nearly-40-from-all-time-high/#1f9a3ae97c74.
3. 'Presenting: Malwarebytes Labs 2017 State of Malware Report'. Malwarebytes Labs, 25 Jan 2018. Accessed May 2018. https://blog.malwarebytes.com/malwarebytes-news/2018/01/presenting-malwarebytes-labs-2017-state-of-malware-report/.
4. 'Enterprise phishing resiliency and defense report 2017'. Cofense. Accessed May 2018. https://cofense.com/whitepaper/enterprise-phishing-resiliency-and-defense-report/.