You Could Be Mine(d): The Rise of Cryptojacking

Domhnall Carlin, Jonah Burgess, Philip O'Kane, and Sakir Sezer | Queen's University

Traditional malicious attacks have evolved beyond file-based methods, with malicious files now existing as processes and services to evade detection. This article examines the rise of cryptojacking—the use of another's machine for profit through cryptocurrency mining—and how we're all at risk.

With the rise in value and popularity of cryptocurrencies, a novel opportunity for both legitimate and illegitimate gain has developed and is currently being exploited on a large scale. The actual cost of cryptomining (i.e., earning cryptocurrency by performing the CPU-intensive calculations that underpin the blockchain technology) can far outweigh the potential income, with the costs of specialist cryptomining machines and the inevitable utility bills yielding a net loss. The balance sheet can be turned profitable by off-loading these costs to a distributed network of machines. While antivirus (AV) solutions can offer a degree of protection against file-based threats, i.e., executable malware, new fileless malicious attacks proffered through the web browser can easily evade current detection techniques. The result is the surreptitious hijacking of a user's CPU for illegitimate gain, and we're only at the tip of the iceberg.

Fileless Malware

A shift in the attack patterns of malware has become evident, moving from file-based to fileless attacks. As AV technology falls behind in this arms race, malware authors are becoming increasingly skilled at finding new attack vectors. It is along these little-known routes that the propagators of malware can usher their code past AV solutions and ultimately earn a tidy profit.

Digital Object Identifier 10.1109/MSEC.2019.2920585
Date of current version: 1 July 2019

Fileless malware (or nonmalware) attacks are simply defined as malicious attacks on a system without the use of a file (e.g., document, executable, jpg) on disk. The adversary uses existing authorized benign software and processes for malicious purposes, without downloading any files to disk.[1] Such software includes the typical applications an average user would employ daily (e.g., web browser, Office, Flash) and utilities purposely residing in the operating system (e.g., PowerShell). The key point is that the files are not committed to disk, not that files are not downloaded. Such script-based malware attacks have increased in the past two years, with as many as 53% of breaches being initiated by nonmalware attacks.[1]

Cryptomining

Mining for cryptocurrency (cryptomining) is not a new phenomenon. For as long as cryptocurrencies, such as Bitcoin, have existed, users have devoted computing resources to mining coins. In fact, the concept of cryptocurrencies very much depends on mining by the user-base. Cryptomining malware is not new either, and when cybercriminals discovered the potential for profit, they began to develop malware that could be used to infect victims and force them to unwittingly mine cryptocurrency on their behalf.

Browser-based cryptomining was first introduced in 2013 with Tidbit. This proof-of-concept was developed by students at the Massachusetts Institute of Technology as a potential alternative to in-browser advertising

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/20©2020IEEE

during a hackathon. Although the students won the "most-innovative" award for the idea, they subsequently received a subpoena from the state of New Jersey. However, their case was later dropped subject to conditions. Notably, at the time of settlement, the state prosecutors conceded that Tidbit did not appear to be developed for malicious purposes.[2]

The concept of browser-based mining lost favor with the continued fluctuation in cryptocurrencies, but the 1,000% increase in Bitcoin value throughout 2017 was closely followed by a similar surge in interest by those hoping to profit through surreptitious coin mining. Off-loading the hardware outlay and operational expenses of dedicated cryptomining machines on to others offers potential profit without overheads. This has even resulted in competition between cryptomining malware strains, with code found in the wild that ejected any miners that were already present on the target host in favor of the newer attacker's mining malware.[3]

Publicly accessible application programming interfaces (APIs) were made widely available at the end of 2017, starting with CoinHive. These can be used intentionally by the service owner, e.g., as a revenue stream, regardless of whether the end user is aware of the event. The mining is normally spawned with trivial JavaScript, which is embedded into the host HTML file as shown in Figure 1.

The code can also be injected maliciously by a third party, with neither the end user nor the website owners being aware. As such, all running and capital costs are borne by the website and user, with the profits going to the miscreant, minus a small percentage for the API provider. It appears evident that this new attack vector is just at the beginning of its evolution. As demonstrated by the explosion in ransomware, the development of technology intended for societal gain can be equally used for criminal profit. However, to date the academic literature on the phenomenon is scarce.

Cryptojacking

The phenomenon of cryptojacking is a relatively new concept. Cryptojacking can be defined as the unauthorized hijacking of the victim's web browser to mine for cryptocurrency (e.g., BitCoin, Monero, Ethereum). The end of 2017 saw a spate of websites engaging users' browsers for cryptomining, following the release of CoinHive. Similar scripts quickly followed, including CoinHave, JSECoin, and CryptoLoot. This could be contrasted with typical ransomware attacks, as the perpetrator is profiting from putting the user's machine to work, rather than out of work. As no files are copied to disk, no signature for the attack exists. As the host software employed is expected and normal, the attack can be invisible to endpoint security solutions. Crucially, no administrator privileges are required for this process to occur.

These scripts drew the attention of the security community, and ad-blocking software began blocking them by default. CoinHive argues that its scripts are legitimate alternatives to advertising revenue, and the responsibility for informing users lies with the site owners. To promote this idea, and to bypass the ad-blockers, CoinHive released AuthedMine, which performs the same actions as the original API, but not until user consent is explicitly gained. This approach has been successful, as AuthedMine is not currently blocked by any ad-blocking or AV product.

Cryptojacking has mushroomed, with an 8,500% increase in prevalence in Q4 of 2017,[4] and it was listed as the top threat for 2018 by MalwareBytes.[5] A combined total earning of US$150,000 per month through more than 1 billion visits by users has been estimated for just 33,000 sites.[6] Almost 90% of remote code execution attacks (i.e., when the attacker can execute arbitrary code via a network connection on a remote machine) on webservers has been attributed to drive-by mining setup,[7] highlighting a shift in payloads and, therefore intentions, from botnets to cryptomining.

By the start of 2018, several high-profile companies became victims of the cryptojacking trend, including Starbucks in Buenos Aires and media giant YouTube. Four online video sites, serving close to 1 billion users monthly, were potentially engaging their users in cryptomining unknowingly.[6] The *Los Angeles Times* website was compromised due to a poorly configured Amazon Web Service and used for drive-by mining, as was Tesla's public cloud service.

In February 2018, 4,263 sites were discovered to be unintentionally cryptojacking their users. A third-party accessibility service for websites was breached, causing each site to instantiate a CoinHive miner on every page load.[8] Due to the nature of the plug-in, many government and public agency websites were affected, including uscourts.gov, many council sites in the United Kingdom and Ireland, the U.K. National Health Service, and, ironically, the U.K. Information Commissioner's Office. Although the attack lasted only approximately 4 h and yielded a meager US$24, it serves to demonstrate the potential of this style of attack across the staggering number of Internet-connected devices.

```
<script src="[redacted]min.js"></script>
   <script>
   CoinHive.CONFIG.WEBSOCKET_SHARDS = [["[redacted]"]];
   var miner = CoinHive.Anonymous('test1', {throttle: 0.4});
   if (!miner.isMobile()) {
       miner.start();
   };
```

Figure 1. An example of the simplicity of CoinHive's implementation.

Eskandari et al.[9] examined the ZMap top 1 million websites and found 30,611 websites to be running CoinHive, with 2,671 sites running other miner families (Figure 2). Following the blocking of CoinHive by AV software and ad-blockers, a repeated search found the same ratio of CoinHive to other miners. AuthedMine was detected on only 60 websites one month after its release, although that figure appeared to be climbing.

Business Model

While CoinHive currently dominates the cryptojacking market, newer alternatives have tried to attract custom by charging lower commission rates than their biggest rival. Brave, a new open source browser, maintains its own cryptocurrency called *Basic Attention Token* (*BAT*). While Brave does not actually cryptomine, it ad-blocks by default, citing the medium as abusive and detrimental to smartphone battery life (by 21%) and site performance (5-s loading time per ad).[10] In return, Brave offers BAT as a reward for continuing to use the ad-blocking feature. There is the potential for websites to offer cryptomining-based rewards for users who consent to their machines being used for cryptomining, such as discounts, credits, exclusive content, and premium features. Cryptojacking also allows sites that are blacklisted from carrying regular ads to generate income, and some websites use cryptojacking along with, rather than in place of, ads.

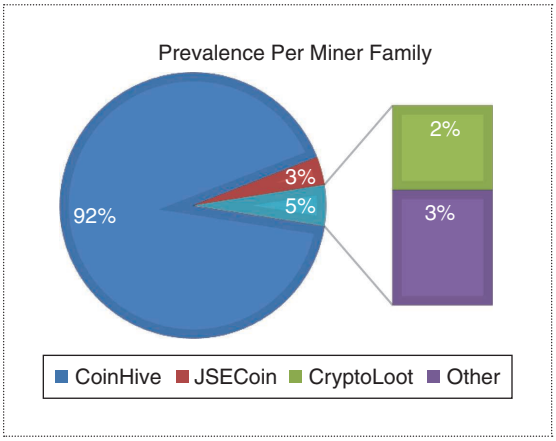

Figure 2. The prevalence of miners per family found in Eskandari et al.[9]

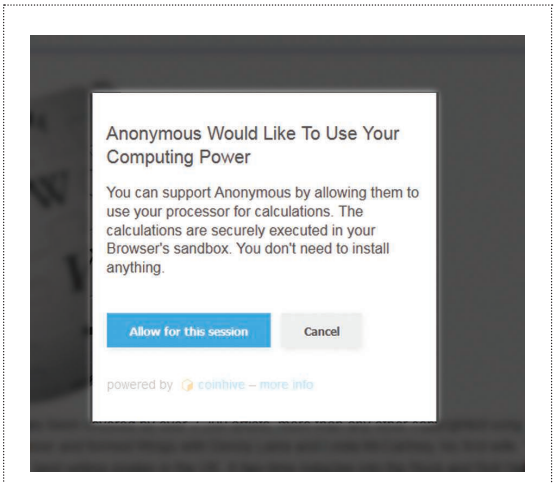

Figure 3. A user notification based on AuthedMine.

Threat Sources

The potential of serving cryptojacking scripts to huge numbers of users by breaching legitimate services presents a highly valuable prize for hackers. The originating sources of cryptojacking scripts can be broken down into three main categories.

Intentional Introduction by Website

Webmasters can integrate a script to implement cryptomining in the user's browser directly into their own website. This is the use-case stated by the script providers, primarily to replace income lost when ads are removed. The option is available to inform the user that this will occur and, further, to seek explicit consent from the user (Figure 3).

Two popular sites caught surreptitiously running CoinHive were Showtime and Ultimate Fighting Championship (UFC). Showtime refused to make a public statement about the discovery, prompting researchers to point out that the occurrence was potentially due to New Relic, a third-party digital insight service (https://twitter.com/bad_packets/status/912386406999252992). However, New Relic denied these accusations, suggesting that the miner was added by Showtime developers. The UFC has denied the existence of the script, and the origin of the miner found on their site remains unknown (https://twitter.com/bad_packets/status/928044219222048769).

Third-Party Services

A huge proportion of websites utilize third-party services, e.g., tracking and analytical tools, JavaScript libraries, and advertisements. This creates an opportunity for coin-mining scripts to be injected into the third-party services, either deliberately by the developers or resulting from a breach. As a result, the scripts are cascaded to all websites that use the service, much like the malvertising attack vector, where poisoned webpage ads are employed to launch attacks, due to their distributed nature. One of several real-world examples of this threat was discovered by researchers at Trend Micro. They detected a rise of 285% in the quantity of implemented CoinHive instances in one single day, determining that

the traffic came from DoubleClick advertisements.[11] In a further example, a plug-in called *LiveHelpNow* was compromised and used to perform mining on around 1,500 sites. PolitiFact, a website devoted to fact-checking U.S. politicians, was compromised via a third-party JavaScript library. This led to CoinHive being executed at 100% CPU usage for an unknown portion of the site's 3.2 million monthly visitors.

Browser Extensions

Browser extensions can present a similar threat to those threats posed by third-party services. If the extension runs a cryptominer, it could potentially generate a large revenue stream. This would not be due to the number of impacted users alone but also because the mining script would be run for as long as the browser itself is open. For the script propagator, this has the distinct advantage of executing the script for any web address, without the need for infecting any. One such example is the popular Chrome extension Archive Poster. This was found to be running a cryptominer on an unknown section of their user base for several days, allegedly due to stolen developer credentials.[12]

> **While closing down the active browser window may be a simple way to terminate many browser-based cryptominers, some miners were found to spawn translucent pop-under windows.**

Implications

As a general rule, increasing devoted computational power increases the mining yield. The desire for increased computational power recently led to the arrest of Russian scientists trying to mine Bitcoin in a nuclear facility. In the context of cryptojacking, this suggests cryptominer implementers are likely to utilize as much CPU power as they can get away with (Figure 4). This is further demonstrated by the lack of throttling, i.e., percentage of CPU resources commandeered, during cryptomining. Although the default setting is 100%, the throttling option is trivially implemented in the CoinHive script. It is also worth noting that the network bandwidth consumption of the mining behavior is minimal, peaking at approximately 3 kb/s within instances we have observed, which is unlikely to draw the attention of users or IT departments.

There are some serious potential consequences of commanding increased computational resources to mine cryptocurrencies. An industrial control system (ICS) security firm reported the discovery of cryptomining malware in the operational technology network of a water utility provider in Europe that was responsible for monitoring and control. This is the first known instance of cryptomining malware directly targeting an ICS, and it used sophisticated antianalysis techniques to thwart detection. This attack had a significant impact on the system and could have caused it to hang or crash, with real-world consequences.

While ICS attacks reach high-impact single targets, there are potentially much more readily available threats. A recent instance of Android malware, Loapi, was discovered on mobile phones. It was being employed to mine Monero so aggressively that it resulted in visible physical damage to the victim's device.[13] Researchers at Kaspersky tested the malware under lab conditions and found that, after only 48 h, the mining had caused the battery to bulge so severely that it caused the case of the phone to warp. It is not difficult to imagine the potentially severe consequences that cryptomining malware could have on mobile devices.

Mitigations

Defenses employed against other types of web-based malware also currently apply to cryptojacking. Security products, such as AV applications, may block the scripts by default. Browser extensions like NoCoin, minerBlock, and NoScripts can prevent the mining scripts from executing, as can many standard ad-blockers. Blacklists can be used to block sites that have been reported to run mining scripts. Many such lists exist publicly and can be easily implemented by users. For example, the Opera browser features a built-in NoCoin blacklist. However, this deals only with currently known services and their

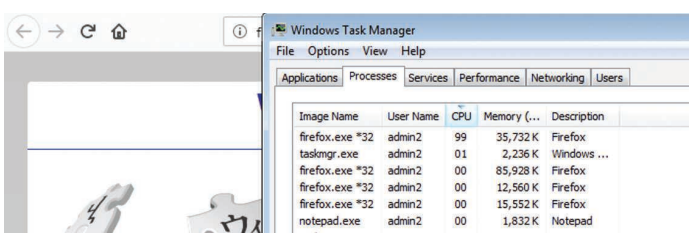

Figure 4. A miner causing Firefox to consume ~99% of CPU resources.

listed domains. There are no known security products or ad-blockers that block the AuthedMine script, suggesting that the scripts are only classified as malicious if user consent is not explicitly sought.

Following the February 2018 BrowseAloud breach, the U.K. National Cyber Security Center advised developers and administrators on cryptojacking mitigation.[14] The main advice issued to website administrators focused on the use of subresource integrity (SRI) and content security policy (CSP) measures. SRI is a hash-based protocol for script checking, allowing a site to validate the integrity of any called scripts. CSP is a whitelisting service for third-party script downloads, allowing control over the domains from which scripts are permitted. However, SRI is not supported in all browsers, and hashing can be rendered redundant by frequently modified scripts.

While closing down the active browser window may be a simple way to terminate many browser-based cryptominers, some miners were found to spawn translucent pop-under windows, keeping the attack active when the user believes that they have closed the browser down.[15] Similarly, preventing miners from running by denying permission for JavaScript can be easily circumvented by WebASM-enabled threats, featured in newer cryptominer samples.

Evasion and Antianalysis Techniques

The evasion and antianalysis techniques employed during cryptojacking are similar to those used by exploit kits (EKs), the automated vulnerability scanners found on compromised webpages and used to mass-distribute exploits. A cryptomining script called *Minr* has already begun to provide automatic code obfuscation and periodically checks blacklists, modifying URLs accordingly.

A further potential evasion technique is the dynamic loading of cryptomining scripts, which may bypass some static web crawlers. It is a trivial task to detect such dynamically loaded scripts, but web pages must be rendered, slowing down crawler-based detectors. Some mining sites have been found to employ proxy servers. This allows the direct loading of cryptomining scripts, rather than from service providers such as CoinHive, therefore bypassing blacklists. It is likely we will see similarly innovative tactics to avoid detection and achieve persistence in the future.

Legality and Ethics

The legality of cryptojacking remains unclear. By not explicitly obtaining consent from the machine owner, or at least informing them of the operation, cryptojacking certainly represents a theft of computing resources.

In the United Kingdom, Section 3 of the Computer Misuse Act (1990) sets out three offenses involving computers:

1. *A person is guilty of an offence if—*
   a. *he does any unauthorised act in relation to a computer;*
   b. *at the time when he does the act he knows that it is unauthorised; and*
   c. *either subsection (2) or subsection (3) below applies.*
2. *This subsection applies if the person intends by doing the act—*
   a. *to impair the operation of any computer;*
   b. *to prevent or hinder access to any program or data held in any computer;*
   c. *to impair the operation of any such program or the reliability of any such data;*
   d. *to enable any of the things mentioned in paragraphs (a) to (c) above to be done.*
3. *This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) to (c) of subsection (2) above.*

However, the key component of the Act is that the person has both intent and is aware that the action is unauthorized. While there does not appear to be a test case for this within the U.K. judicial system yet, cryptojacking may indeed be a breach of this Act.

In the United States, the relevant law is Title 18 of the U.S. Code, § 1030: "Fraud and related activity in connection with computers." Section A, Article 5 states that is an offense for a person who:

A. *knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;*
B. *intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or*
C. *intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.*

While "protected computer" is limited by definition as a computer for the exclusive use of a financial institution or the U.S. government, or one that is used in or affects interstate or foreign commerce or communication, this definition has been expanded to cover almost any computer connected to the Internet (see United States v. Macewan[16]). However, Article 4 states that an offense is committed if the person:

4. *knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained*

consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

Although, if the object of the fraudulent activity is the use of the machine, and the value is below US$5,000, no offense is committed.

The legal status of cryptojacking, with or without the user's express permission, remains unclear. With the rapid rise in the deployment of such surreptitious miners, it is probable that case law will soon catch up with the technology.

Ethically speaking, cryptojacking is a gray area. It is apparent that cryptojacking resulting from a breach is both unethical and illegal. There is a general consensus that, in the absence of user awareness or consent, the process is clearly unethical. Even with explicit consent, some users may not understand what it is that they are granting permission for and what they are receiving in return. Support for the use of cryptomining scripts as alternatives to ads has found some favor among users. This could increase if sites begin to offer user-specific rewards, such as premium content and features.

It may, in fact, be the case that cryptojacking could help overall web security, by reducing the threat posed by ads. Malvertising is often used to expose users to threats such as EKs, which can distribute malware rapidly. Therefore, if cryptojacking is made a legitimate and viable alternative to advertising, through user permissions and responsible implementations, it may be a safer mechanism for the user, while maintaining income for the owner.

Cryptojacking has already had a massive impact on the online world and, with the seemingly unending development of connected smart devices, it is not hard to envisage a rapid escalation of cross-platform attacks. With the readily available APIs that allow cryptojacking to be implemented with ease, it is important for individuals to be made aware of the theft of their resources and allowed the opportunity to give informed consent. This may even have beneficial aspects, allowing websites to maintain revenue and users to avoid the risks inherent with online advertisements. Research at the Centre for Secure Information Technologies is focusing on the development of a platform for scanning a website for known cryptomining threats, which have been compiled through observation of thousands of cryptojacking sites. Tens of millions of sites are scanned daily, with the results compiled into a central database. This will be the first major step in defending our privacy, security, and trust against this new threat. ■

References

1. M. Viscuso, "What is a non-malware (or fileless) attack?" Carbon Black, Feb. 10, 2017. Accessed on: Feb. 1, 2018. [Online]. Available: https://www.carbonblack.com/2017/02/10/non-malware-fileless-attack/
2. Electronic Frontier Foundation, "Rubin v. New Jersey (Tidbit)," Feb. 3, 2014. [Online]. Available: https://www.eff.org/cases/rubin-v-new-jersey-tidbit
3. X. Mertens, "The crypto miners fight for CPU cycles," SANS Internet Storm Center, Mar. 4, 2018. [Online]. Available: https://isc.sans.edu/forums/diary/The+Crypto+Miners+Fight+For+CPU+Cycles/23407
4. S. Liao, "Cryptojacking rates increased by 85 times in Q4 2017 as bitcoin prices spiked: Report," The Verge, Mar. 22, 2018. [Online]. Available: https://www.theverge.com/2018/3/22/17147320/cryptojacking-8500-percentage-points-bitcoin-monero-spike-symantec-security-mining
5. Malwarebytes, "Malwarebytes reveals 2018 security predictions," Nov. 20, 2017. [Online]. Available: https://press.malwarebytes.com/2017/11/20/malwarebytes-reveals-2018-security-predictions/
6. A. Meshkov, "Crypto-streaming strikes back," AdGuard, Dec. 13, 2017. [Online]. Available: https://adguard.com/en/blog/crypto-streaming-strikes-back.html
7. N. Avital and G. Yehudai, "New research: Crypto-mining drives almost 90% of all remote code execution attacks," Imperva, Feb. 20, 2018. [Online]. Available: https://www.imperva.com/blog/new-research-crypto-mining-drives-almost-90-remote-code-execution-attacks/
8. S. Helme, "Protect your site from cryptojacking with CSP + SRI," scotthelme.co.uk, Feb. 11, 2018. [Online]. Available: https://scotthelme.co.uk/protect-site-from-cryptojacking-csp-sri/
9. S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark, A first look at browser-based cryptojacking. Mar. 2018. [Online]. Available: https://arxiv.org/abs/1803.02887
10. Brave Software, "Basic attention token (BAT): Blockchain based digital advertising," Brave Software, San Francisco, CA, White Paper, 2018. [Online]. Available: https://github.com/brave-intl/basic-attention-token-crowdsale/raw/master/whitepaper/Basic AttentionTokenWhitePaper.pdf
11. C. Liu and J. C. Chen, "Malvertising campaign abuses Google's DoubleClick to deliver cryptocurrency miners," TrendMicro, Jan. 26, 2018. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/
12. J. Segura, "The state of malicious cryptomining." Malware Bytes, 2018. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/
13. D. Goodin, "Currency-mining Android malware is so aggressive it can physically harm phones," Ars Technica,

Dec. 19, 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/12/currency-mining-android-malware-is-so-aggressive-it-can-physically-harm-phones/

14. National Cyber Security Centre, "NCSC advice: Malicious software used to illegally mine cryptocurrency," Feb. 11, 2018. [Online]. Available: https://www.ncsc.gov.uk/guidance/ncsc-advice-malicious-software-used-illegally-mine-cryptocurrency
15. J. Segura, "Persistent drive-by cryptomining coming to a browser near you," Malwarebytes, Nov. 29, 2017. [Online.] Available: https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/
16. U.S. Court of Appeals, 3rd Circuit. (2006 Apr. 5). *No. 05-1421, United States of America v. James E. Macewan, Appellant*. [Online]. Available: https://caselaw.findlaw.com/us-3rd-circuit/1313851.html

Domhnall Carlin is a research fellow at the Centre for Secure Information Technologies at Queen's University, Belfast, Northern Ireland, where he received a Ph.D. in computer science. His research interests include machine learning for low-level malware analysis.

Jonah Burgess is a Ph.D. candidate at the Centre for Secure Information Technologies at Queen's University, Belfast, Northern Ireland. After completing modules taken from the M.Sc. in cybersecurity, he is now focusing on web- and browser-based threats.

Philip O'Kane is a lecturer at the Centre for Secure Information Technologies at Queen's University, Belfast, Northern Ireland, where he received a Ph.D. for his work on the detection of obfuscated malware. He started his career as an embedded software engineer in the telecommunication industry and later moved to application development for the finance industry. He has 20 years of experience in software development in industry. His research interests include the low-level analysis and detection of malware.

Sakir Sezer is a professor and the head of network and cybersecurity research at the Centre for Secure Information Technologies at Queen's University, Belfast, Northern Ireland. His research focus is leading major advances in the field of high-performance content and security.

Digital Object Identifier 10.1109/MSEC.2020.2975969