QBot: Laying the Foundations for Black Basta Ransomware Activity

reliaquest.com/blog/qbot-black-basta-ransomware/

March 15, 2023

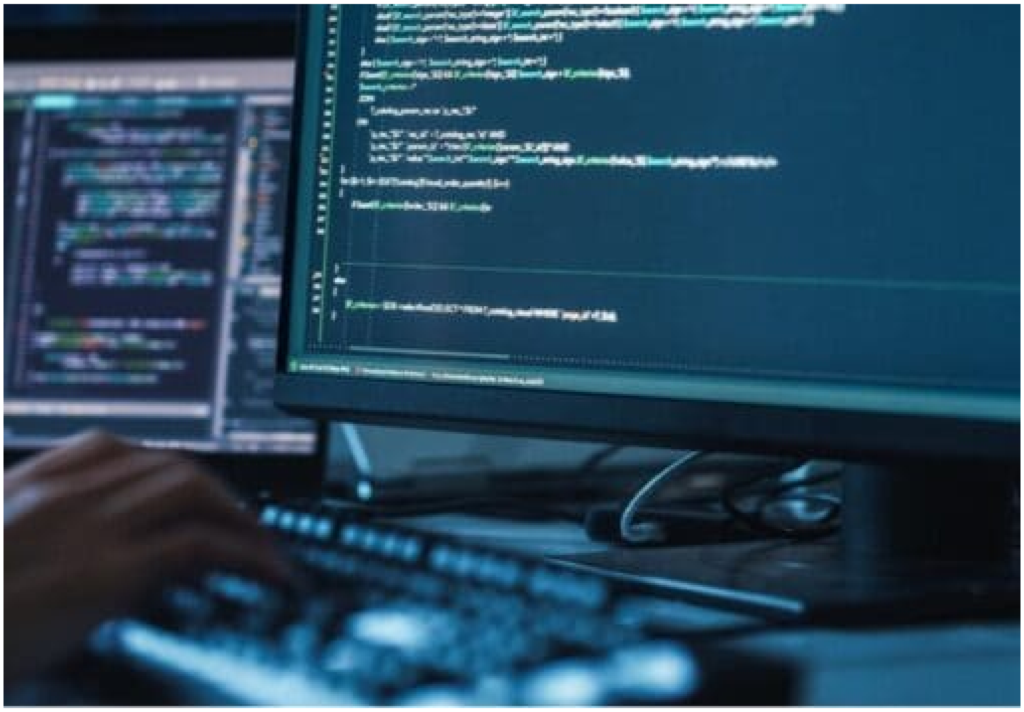


Table of Contents

Toward the latter half of Q4 2022, ReliaQuest discovered a security incident unfolding in a customer's environment. A threat actor gained initial network access, rapidly escalated their privileges, and moved laterally, quickly establishing a foothold in 77 minutes.

We severed the foothold the adversary established and worked alongside the impacted customer to remediate the implications of the intrusion, but some valuable lessons should be taken away: many of the attackers' actions were assisted by an accepted risk that, if avoided, could have prevented—or at least slowed—their advances.

The threat actors' techniques—notably the use of "QBot" for initial access—suggested they are an affiliate of the "Black Basta" ransomware-as-a-service (RaaS) program. Ransomware remains, arguably, the most pernicious threat that businesses face in 2023. Let's go over some simple changes that can often mean the difference between remediation and catastrophe.

Download the Q1 2023 Ransomware Report >

What Is QBot?

Also known as Qakbot, QuackBot, and Pinkslipbot, QBot is a banking trojan that was first observed in 2007. As observed with other prominent banking trojans, like “Emotet,” QBot has come to acquire many new functions and is consistently being developed to incorporate new techniques and capabilities. In addition to stealing financial details and personally identifiable information (PII), QBot can be used for lateral movement, detection evasion and debugging, and installing additional malware on compromised machines.

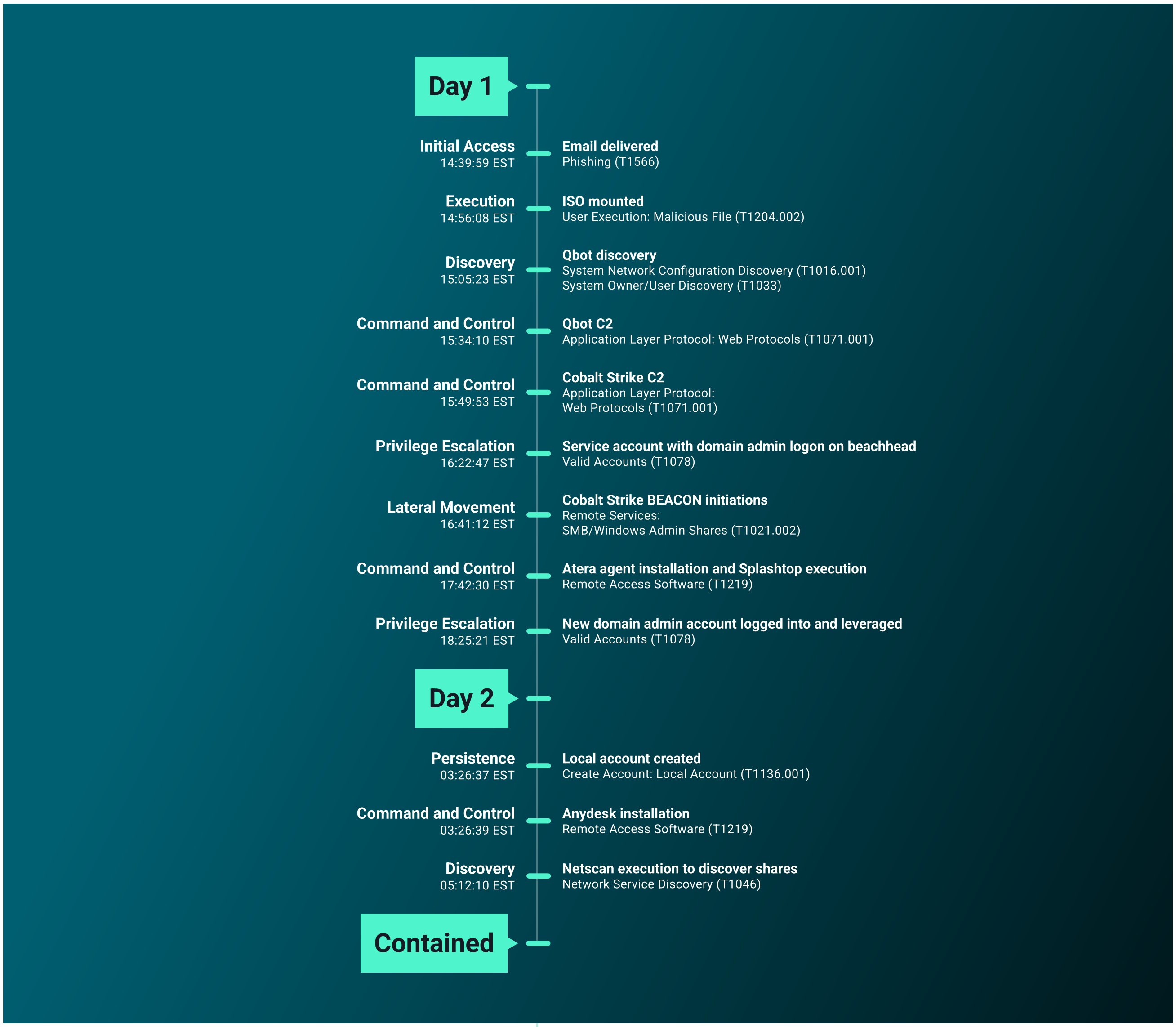
Attack Overview: Stealth and Swiftness

On September 29, 2022, we detected malicious activity after the deployment of Cobalt Strike Beacon and remote management software in a customer’s environment. The attacker achieved initial access via a phishing email delivered to end-user inboxes—having slipped past an overly permissive security solution.

This phishing email led to the deployment of the QBot malware and gave the attacker an initial foothold in the environment. They obtained valid service account credentials that were part of a domain administrator group, smoothing the path to move laterally and deploy other Cobalt Strike beacons.

The timeline of initial QBot execution to lateral movement, commonly known as the breakout time, was 77 minutes. (See Figure 1 for a timeline.) This is far quicker than most cases of this kind, which usually have a breakout time of around 2 hours.

The attacker’s actions had the whiff of a Black Basta affiliate, with Qbot activity widely reported as being a cornerstone of Black Basta intrusions. Black Basta is a splinter group that emerged after the “Conti” ransomware syndicate was quelled; its members moved on to alternative ransomware programs. The Black Basta group operates a ransomware-as-a-service (RaaS) program.



Day 1

Initial Access 14:39:59 EST — **Email delivered** Phishing (T1566)

Execution 14:56:08 EST — **ISO mounted** User Execution: Malicious File (T1204.002)

Discovery 15:05:23 EST — **Qbot discovery** System Network Configuration Discovery (T1016.001) System Owner/User Discovery (T1033)

Command and Control 15:34:10 EST — **Qbot C2** Application Layer Protocol: Web Protocols (T1071.001)

Command and Control 15:49:53 EST — **Cobalt Strike C2** Application Layer Protocol: Web Protocols (T1071.001)

Privilege Escalation 16:22:47 EST — **Service account with domain admin logon on beachhead** Valid Accounts (T1078)

Lateral Movement 16:41:12 EST — **Cobalt Strike BEACON initiations** Remote Services: SMB/Windows Admin Shares (T1021.002)

Command and Control 17:42:30 EST — **Atera agent installation and Splashtop execution** Remote Access Software (T1219)

Privilege Escalation 18:25:21 EST — **New domain admin account logged into and leveraged** Valid Accounts (T1078)

Day 2

Persistence 03:26:37 EST — **Local account created** Create Account: Local Account (T1136.001)

Command and Control 03:26:39 EST — **Anydesk installation** Remote Access Software (T1219)

Discovery 05:12:10 EST — **Netscan execution to discover shares** Network Service Discovery (T1046)

Contained

Kill Chain Details: Where Did It All Go Wrong?

Initial Access

The phishing email that granted initial access was delivered on 26 Sep 2022. The attachment to the message was named **REF#6547_SEP_28.HTML**, which was rightly detected by Office 365 management as malicious: It was smuggling a ZIP file onto the targeted network, to deliver a QBot implant. The email's content prompted the recipient to look at the attached file and approve its content.

Execution

Execution was achieved by HTML smuggling. Upon opening the HTML file in an email client, the screen pictured in Figure 2 was shown and the user was asked to download it locally. After they did so and opened the HTML file in a browser, an encoded JavaScript binary large object (BLOB) surfaced. The BLOB then constructed and automatically downloaded a ZIP file to the user's disk.

Figure 2: Fake Adobe Acrobat update

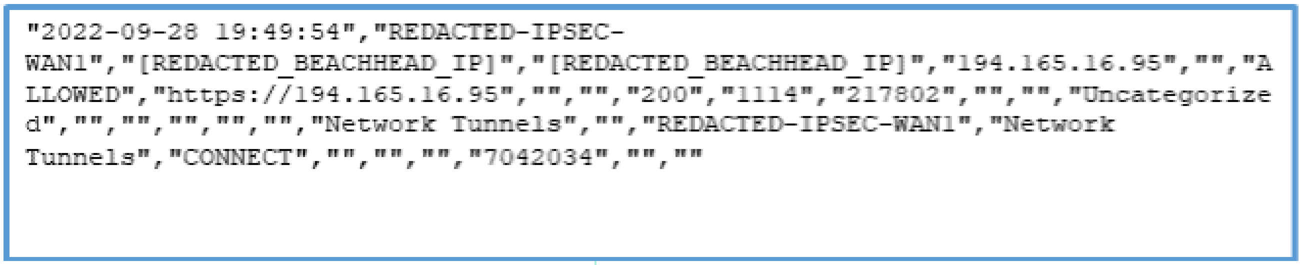
The ZIP file was protected by the password that then appeared on the screen: `abc333`. Once opened, an ISO image was found within the zipped archive; if double-clicked, the ISO was mounted to disk. Within the new drive—which is created when the ISO is mounted—was a LNK file, which pointed at a JS file which in turn invokes script `STICKLERBLOWN.CMD`. Of course, this all starts with the user clicking on that LNK file.

This concluded the current QBot delivery chain, with QBot acting as both trojan and malware dropper to enable an initial foothold onto a target's environment. Fake Adobe Acrobat updates have long been synonymous with the spread of malware, so nothing new here, but it continues to be effective as the software is free and widely used.

In this case, the attacker used the initial QBot foothold to deliver a Cobalt Strike beacon to the beachhead. Cobalt Strike and post-exploitation tools are typical follow-on payloads resulting from these infections. Often, commodity malware is used before moving on to a command-and-control (C2) implant of the attacker's choosing to solidify their foothold on the network.

Command-and-Control

At this point, the threat actor pivoted from the QBot C2 channel to their newly established C2 channel provided by the Cobalt Strike beacon. It was an HTTPS beacon that communicated with its team server located at **194.165.16[.]95**, similar to in other QBot campaigns of RaaS affiliates and initial access brokers (IABs). (We've written before about the increasing role of IABs in facilitating cybercrime.)



```
"2022-09-28 19:49:54","REDACTED-IPSEC-
WAN1","[REDACTED_BEACHHEAD_IP]","[REDACTED_BEACHHEAD_IP]","194.165.16.95","","A
LLOWED","https://194.165.16.95","","","200","1114","217802","","","Uncategorize
d","","","","","","Network Tunnels","","REDACTED-IPSEC-WAN1","Network
Tunnels","CONNECT","","","","7042034","",""
```

The attacker also used alternative HTTPs channels to communicate and maintain their foothold. They deployed and configured remote-access software AnyDesk, Atera, and Splashtop, which use the HTTPS protocol.

The use of commercial remote access software is common. Threat actors associated with Conti ransomware's affiliate program often use Atera and AnyDesk. In this case, AnyDesk was installed following the identification and containment of Atera agents, which had been deployed to multiple compromised hosts. These agents were linked to email address **UQUISKISESHLM[at]GMAIL[.]COM**, which appears to be a random mix of letters; this was most likely conducted for OPSEC purposes.

Credential Access

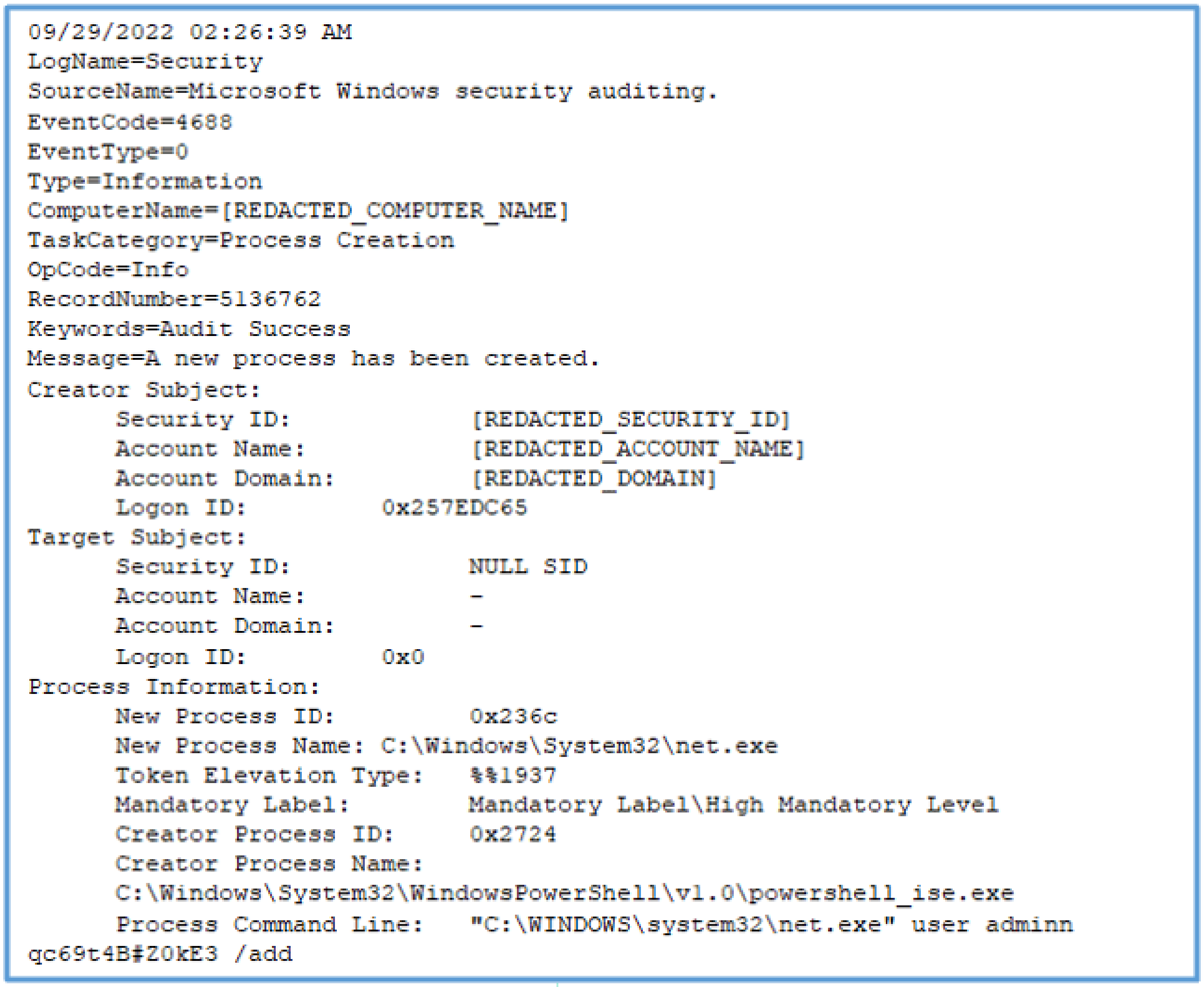
Credential access was achieved after the threat actor used the Data Protection Application Programming Interface (DPAPI) to interact with a credential key for an account; DPAPI is used to protect personal data on the local system, including user credentials. This is a common target for credential harvesting, and in this case, it resulted in the account being compromised. Some of the most common tools—including Mimikatz which was also used during the incident—provide ways to interact with DPAPI to access credentials; Mimikatz is an open-source malware program used by hackers and penetration testers to gather credentials on Windows computers

Privilege Escalation and Persistence

During the intrusion, the attacker primarily made use of a service account with domain administrator privileges. It freed them to carry out objectives until the account was disabled, at which point the attacker pivoted to another valid account that was also a member of the domain administrators' group. This quick pivot upon disabling their primary account was notable.

We were also able to identify another operation which highlights on the theme that the attacker liked to have several available options. We identified that the threat actor attempted to add an account named **OLDADMINISTRATOR** to the Local Administrators group, on hosts where a local account named **ADMINN** had been previously created. We never identified a further account creation for the account **OLDADMINISTRATOR**, which appeared odd. In the Conti affiliate manual, the affiliate is told to create the account **OLDADMINISTRATOR** with the password **qc69t4B#Z0kE3** and then add that account to the Local Administrators group. What the actor did in this case is mistakenly attempted to add the account they were supposed to add to the Local Administrators group. Since the **OLDADMINISTRATOR** had not been created, this was ultimately unsuccessful.

Of all the details we uncovered, this was perhaps the most comical. Even with a playbook, human error is still inevitable. It was also somewhat surprising that Conti's affiliates clearly follow the step-by-step rulebook to a T, even using predesignated passwords.

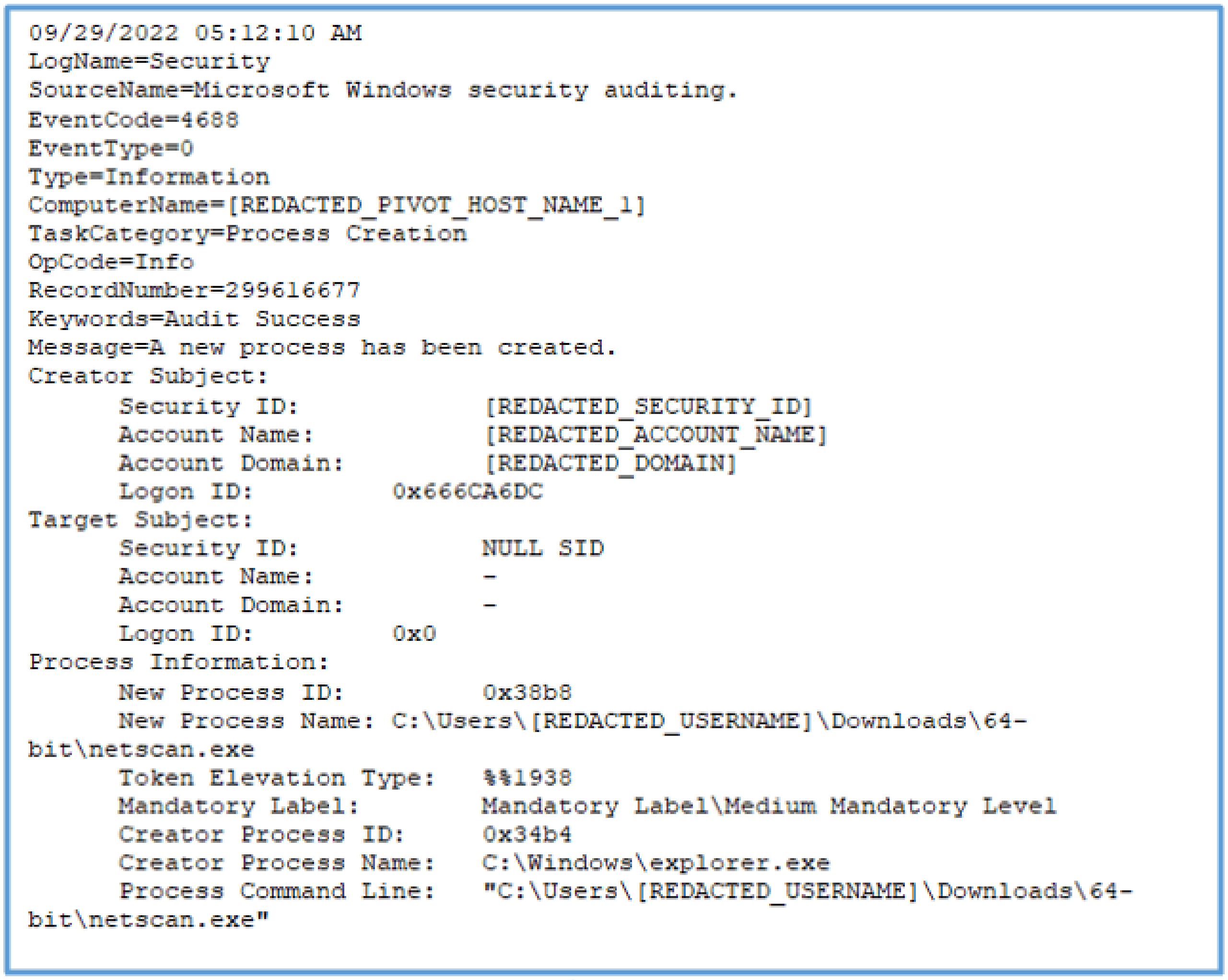


```
09/29/2022 02:26:39 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4688
EventType=0
Type=Information
ComputerName=[REDACTED_COMPUTER_NAME]
TaskCategory=Process Creation
OpCode=Info
RecordNumber=5136762
Keywords=Audit Success
Message=A new process has been created.
Creator Subject:
      Security ID:            [REDACTED_SECURITY_ID]
      Account Name:           [REDACTED_ACCOUNT_NAME]
      Account Domain:         [REDACTED_DOMAIN]
      Logon ID:         0x257EDC65
Target Subject:
      Security ID:            NULL SID
      Account Name:           -
      Account Domain:         -
      Logon ID:         0x0
Process Information:
      New Process ID:         0x236c
      New Process Name: C:\Windows\System32\net.exe
      Token Elevation Type:   %%1937
      Mandatory Label:        Mandatory Label\High Mandatory Level
      Creator Process ID:     0x2724
      Creator Process Name:
      C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
      Process Command Line:   "C:\WINDOWS\system32\net.exe" user adminn
gc69t4B#Z0kE3 /add
```

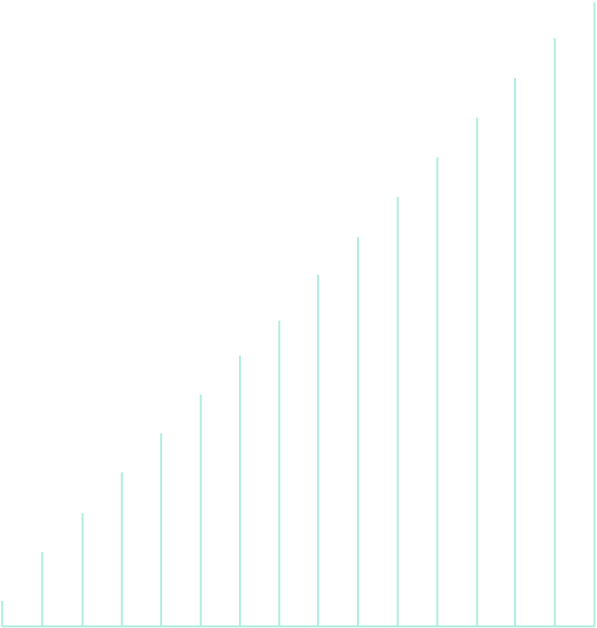
Discovery

Windows binaries were used for network discovery including NET, ARP, ROUTE, NETSTAT, IPCONFIG, and WHOAMI; these were also seen as children processes of WERMGR.EXE. In this case, the Qbot infection was responsible for these discovery operations as the Qbot payload was being run in a memory space of the wermgr.exe process.

We also identified the attacker making use of a networking scanning tool later during this intrusion. The attacker was seen using the tool **NETSCAN.EXE**, which can scan hosts within the network for accessible network shares—another tool known to be used by Conti affiliates.

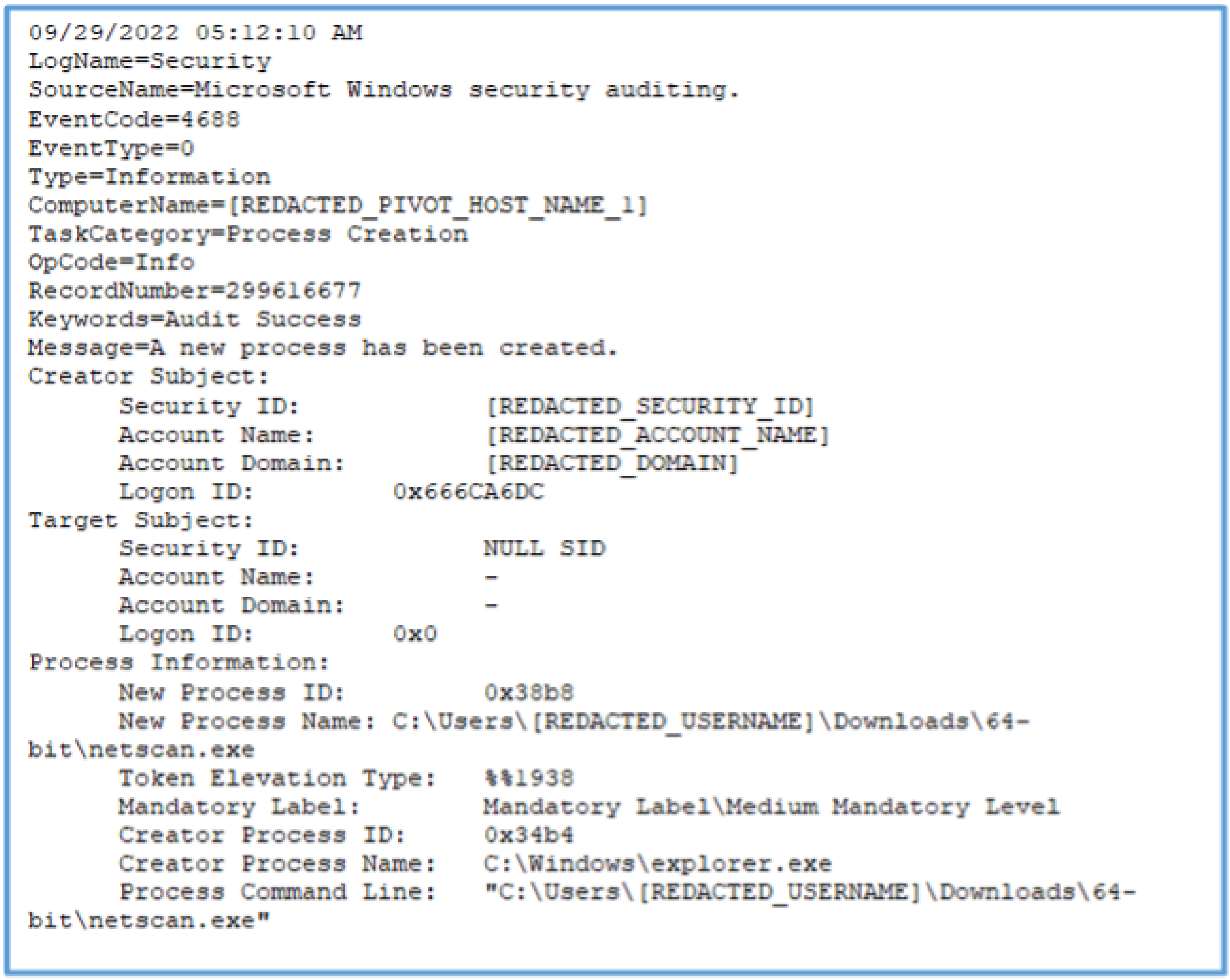


```
09/29/2022 05:12:10 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4688
EventType=0
Type=Information
ComputerName=[REDACTED_PIVOT_HOST_NAME_1]
TaskCategory=Process Creation
OpCode=Info
RecordNumber=299616677
Keywords=Audit Success
Message=A new process has been created.
Creator Subject:
      Security ID:            [REDACTED_SECURITY_ID]
      Account Name:           [REDACTED_ACCOUNT_NAME]
      Account Domain:         [REDACTED_DOMAIN]
      Logon ID:         0x666CA6DC
Target Subject:
      Security ID:            NULL SID
      Account Name:           -
      Account Domain:         -
      Logon ID:         0x0
Process Information:
      New Process ID:         0x38b8
      New Process Name: C:\Users\[REDACTED_USERNAME]\Downloads\64-
bit\netscan.exe
      Token Elevation Type:   %%1938
      Mandatory Label:        Mandatory Label\Medium Mandatory Level
      Creator Process ID:     0x34b4
      Creator Process Name:   C:\Windows\explorer.exe
      Process Command Line:   "C:\Users\[REDACTED_USERNAME]\Downloads\64-
bit\netscan.exe"
```



Lateral Movement

To move laterally, the attacker established remote desktop protocol (RDP) connections, including hijacking active RDP sessions on targeted hosts. They did this by using **QUSER.EXE**: a binary that can enumerate active RDP sessions on devices and identify new users in an environment. Some hijacking attempts failed, and some were successful.

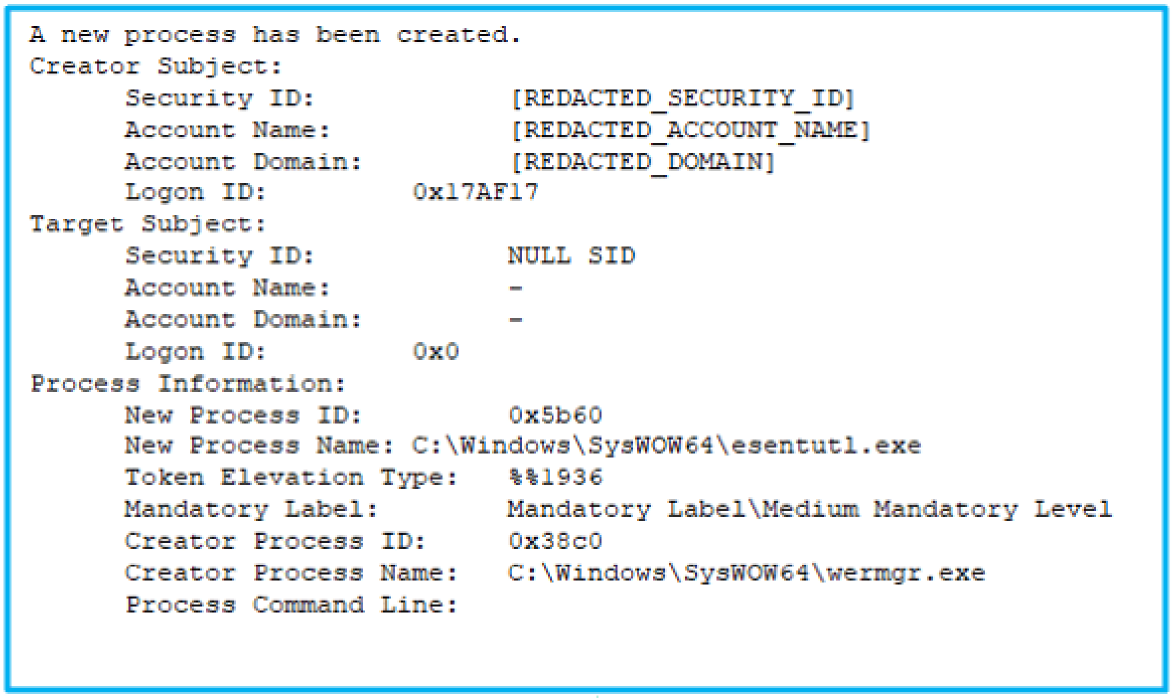


```
09/29/2022 05:12:10 AM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=4688
EventType=0
Type=Information
ComputerName=[REDACTED_PIVOT_HOST_NAME_1]
TaskCategory=Process Creation
OpCode=Info
RecordNumber=299616677
Keywords=Audit Success
Message=A new process has been created.
Creator Subject:
      Security ID:            [REDACTED_SECURITY_ID]
      Account Name:           [REDACTED_ACCOUNT_NAME]
      Account Domain:         [REDACTED_DOMAIN]
      Logon ID:         0x666CA6DC
Target Subject:
      Security ID:            NULL SID
      Account Name:           -
      Account Domain:         -
      Logon ID:         0x0
Process Information:
      New Process ID:         0x38b8
      New Process Name: C:\Users\[REDACTED_USERNAME]\Downloads\64-
bit\netscan.exe
      Token Elevation Type:   %%1938
      Mandatory Label:        Mandatory Label\Medium Mandatory Level
      Creator Process ID:     0x34b4
      Creator Process Name:   C:\Windows\explorer.exe
      Process Command Line:   "C:\Users\[REDACTED_USERNAME]\Downloads\64-
bit\netscan.exe"
```

By investigating events surrounding the failed RDP connections, we saw that the threat actor was accessing administrative shares; admin shares give system administrators remote access to every disk volume on a network-connected system. These shares included the IPC$ network share, which was likely used to establish a remote procedure call (RPC) or server message block (SMB) session. Again, this move was probably made to enable lateral movement.

Collection and Exfiltration

For collection, the threat actor used QBot to start the process **ESENTUTL.EXE**, which is a Living off the Land binary (LOLBin) that provides copy functionality. QBot is known to harvest email data, but whether it did in this case isn't known: A lack of command-line arguments in the host's Windows event logs meant verification wasn't possible.



```
A new process has been created.
Creator Subject:
      Security ID:            [REDACTED_SECURITY_ID]
      Account Name:           [REDACTED_ACCOUNT_NAME]
      Account Domain:         [REDACTED_DOMAIN]
      Logon ID:         0x17AF17
Target Subject:
      Security ID:            NULL SID
      Account Name:           -
      Account Domain:         -
      Logon ID:         0x0
Process Information:
      New Process ID:         0x5b60
      New Process Name: C:\Windows\SysWOW64\esentutl.exe
      Token Elevation Type:   %%1936
      Mandatory Label:        Mandatory Label\Medium Mandatory Level
      Creator Process ID:     0x38c0
      Creator Process Name:   C:\Windows\SysWOW64\wermgr.exe
      Process Command Line:
```

Although ransomware operators are known to prioritize data exfiltration during intrusions, we didn’t find any evidence that this attacker stole data. We did find outbound connections to Cobalt Strike infrastructure (IP address 194.165.16[.]95), but they were likely for typical C2 traffic, rather than being conduits for exfiltrating data. No other tools commonly used for data exfiltration turned up during our investigation.

Defense Evasion

Throughout the event, this attacker used several defense evasion techniques including compressing an email payload, overpass the hash, and process injection. The threat actor archived the QBot payload into a disk image (ISO) file, and then compressed the disk image into a password-encrypted ZIP file to evade email security and Mark of the Web (MotW) controls implemented by Microsoft. They managed this by compressing the payload into a ZIP file-ISO image combination.

This threat actor also performed a sub-technique of pass the hash, known as overpass the hash: passing a targeted account's New Technology LAN Manager (NTLM) hash to the Kerberos authentication provider, resulting in a successful Kerberos authentication.

Process injection was used by both the initial QBot payload (into WERMGR.EXE) and the subsequent deployment of Cobalt Strike (into WERFAULT.EXE).

Process Injection inserts arbitrary code into the address space of another process, giving the appearance that the injected (malicious) code was performed by a normal system process. This evades static detection and application control solutions.

Black Basta's Conti-Linked Heritage

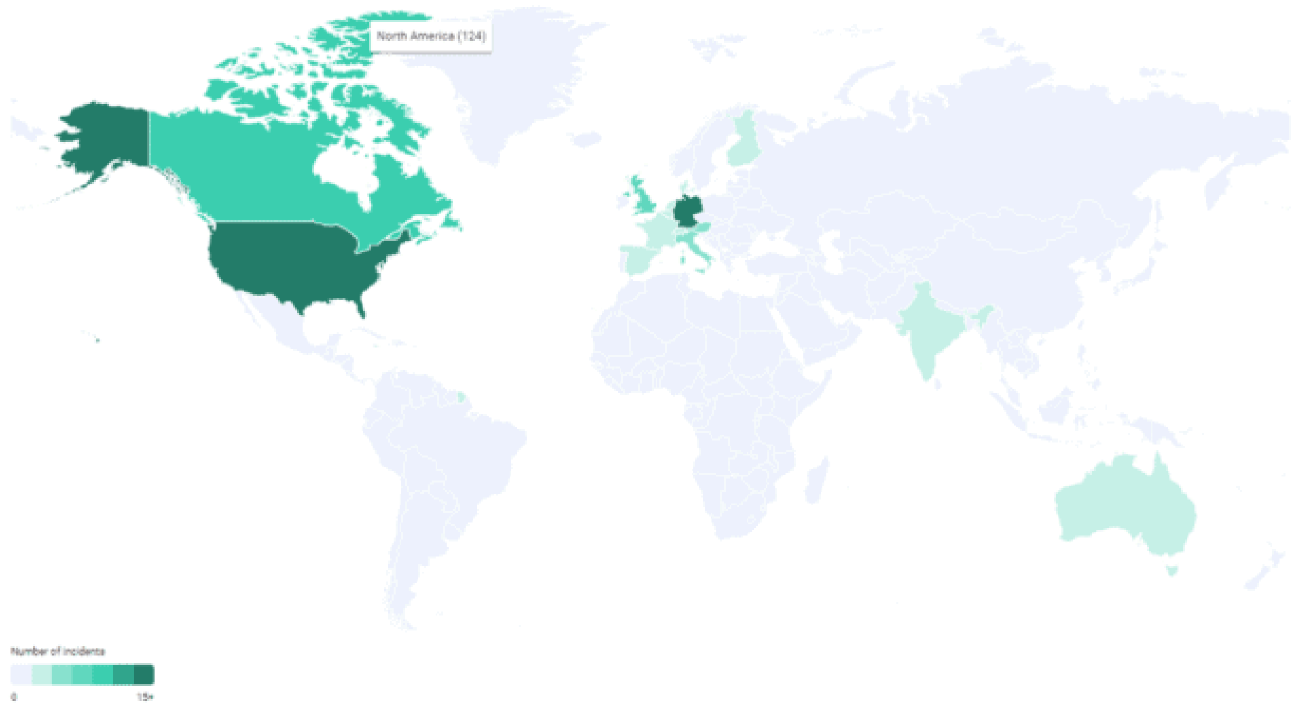
After emerging in 2019, the Conti ransomware group became a top-tier ransomware group before collapsing in May 2022. The demise likely stemmed from a series of operational errors that led to a compromise of Conti's infrastructure.

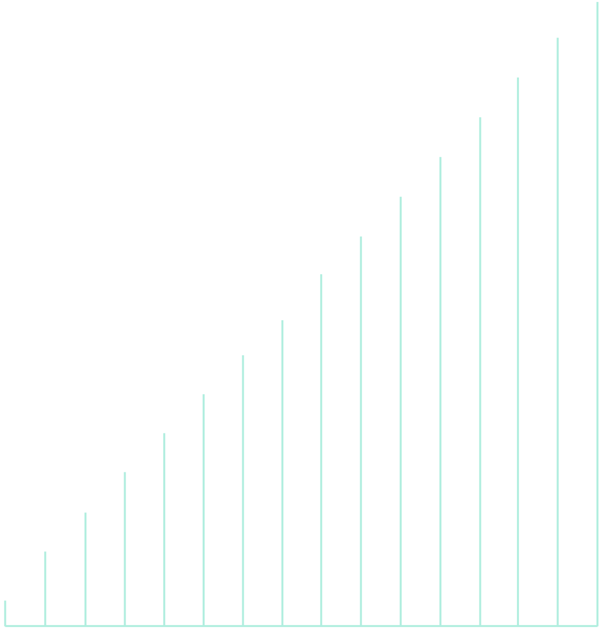
Chat logs taken from Conti were a treasure trove of intelligence for law enforcers and security researchers alike. (You might remember our previous blog exploring five lessons from the Conti breach.) The release of the chat logs also coincided with several other high-profile faux-pas by the group. These included supporting the Russian state during the onset of the war with Ukraine, and also revealed major attacks against the Costa Rican government.

Conti Splinters, Members Move On

As part of Conti's splintering, many members unsurprisingly sought new employment in other ransomware groups. LockBit—which now accounts, overwhelmingly, for the largest market share of ransomware activity—was among the groups that probably welcomed a new intake of members from Conti. Several other groups have also reportedly splintered from Conti , notably the "Karakurt Hacking Team," the "Royal" ransomware group, and Black Basta—those infamous actors attributed to this security incident.

Black Basta first emerged in April 2022, a month before Conti folded. As most major ransomware groups do, Black Basta uses double-extortion to solicit ransom payments, posting stolen data to its Basta News data-leak site if payment is not received within seven days. Black Basta is known to target a wide variety regions and sectors, but mainly construction and industrial goods and services in the US and Germany.





Black Basta Forecast: Stormy Weather

What’s the future for Black Basta and similar splinter groups? Well it’s likely that they’ll encounter increasing scrutiny from governments and law enforcement agencies. On 02 Feb 2023, the UK National Crime Agency and the US Department of the Treasury’s Office of Foreign Assets Control sanctioned seven individuals allegedly involved with Conti and “TrickBot” malware activity. Their real names, birthdates, email addresses, and photos were made public and their lives restricted. This is the first time the UK has sanctioned individuals involved with ransomware, and it’s not likely to be the last.

Those sanctions are part of a wider campaign, portending more arrests, disruptions, and infrastructure take-downs by international law enforcement in the next one to three months. It’s unlikely to have any direct impact on ransomware operations, but it’s the kind of scrutiny that often leads to the closure of threat groups—and the ever-predictable “whack-a-mole” effort to tackle ransomware. (Once a group goes down, you just know they’ll return in some fashion.) If Black Basta members are named and shamed in future sanctions or arrests, we might see another round of ransomware rebranding.

MITRE TTPs

During the course of our investigation, we identified the threat actor using the following TTPs.

Kill Chain Phase	MITRE TTP
Initial Access	Phishing (T1566)
Execution	User Execution: Malicious Image (T1204.003)
Execution	System Services: Service Execution (T1569.002)
Command and Control	Ingress Tool Transfer (T1105)
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)
Command and Control	Protocol Tunnelling (T1572)
Command and Control	Remote Access Software (T1219)
Credential Access	Credentials From Password Stores (T1555)
Privilege Escalation	Valid Accounts (T1078)
Persistence	Create Accounts: Local Account (T1136.001)
Discovery	System Network Connections Discovery (T1049)
Discovery	Network Share Discovery (T1018)
Lateral Movement	Remote Services: remote Desktop Protocl (T1021.001)
Lateral Movement	Remote Services: SMB/Windows Admin Shares (T1021.002)
Lateral Movement	Remote Service Session Hijacking: RDP Hijacking (T1536.002)
Collection	Data From Local System (T1005)

Defense Evasion	Subvert Trust Controls: Mark-of-the-Web Bypass (T1553.005)
Defense Evasion	Use Alternate Authentication Material: Pass the Hash (T1550.002)
Defense Evasion	Process Injection (T1055)

Retaining Ransomware Resilience

Visibility is one of the key ways organizations can minimize the risks posed by the abundant active cyber threats in 2023. You can't secure what's invisible to your incident responders, so ensuring effective logging coverings your assets is essential to detecting and responding to threats. The lack of logs forwarded to the SIEM meant ReliaQuest needed forensics images and event log exports to fill in most of the events in this incident. We've written before about the importance of maximizing business insights by improving logging activities.

Other steps you can take to avoid being impacted by QBot or ransomware activity are as follows.

- Harden perimeter security to restrict company assets from making arbitrary connections to the internet. This may be accomplished through firewall or proxy configurations. This will minimize malware and command-and-control (C2) activity.
- Limit use of remote-access software. This software is one of the most common methods for cybercriminals—notably initial access brokers (IABs) and ransomware operators—to gain access to targeted networks. Consider minimizing the use of such software unless absolutely required for an individual for their jobs. The use of such technology should also be placed under enhanced monitoring to detect any misuse.
- Disable ISO mounting. ISO Mounting is increasingly being used as a method of bypassing anti-virus and endpoint detection tools. Consider disabling ISO mounting by adding the registry key referenced below, which removes the context menu for users when right clicking. This can also be added to your Group Policy to provide protection to all users, while still allowing administrators to mount drives with PowerShell and the Mount-DiskImage command. `HKEY_CLASSES_ROOT\Windows.IsoFile\shell\mount called ProgrammaticAccessOnly`
- Ensure the security of backups and regularly test them for reliability. The "3-2-1" rule is one of the most tried and tested rules for backups, this guideline states that organizations should keep three backup copies, across two different mediums, with one stored off-site. Many businesses may use a combination of the cloud and physical storage to facilitate this requirement. This is also arguably the most secure way to back up data and avoids the risk of backups that are stored on NAS or other network-storage devices being corrupted during a ransomware attack.

ReliaQuest provides a “detection-in-depth” approach to attack coverage, which relies on proper logging being in place. This can be achieved by engaging with our GreyMatter platform, which provides a unified detection-investigation-response process, greatly increasing visibility of the various threats across your attack surface. Having better visibility into threats reduces complexity and helps efficiently manage risk for your business.

The Q1 2023 Ransomware Report

This report looks at the most important ransomware-related events during Q1 2023: key events, metrics of ransomware groups, and what steps organizations can take to protect themselves from these threats.

Get the Report