UNC215: Spotlight on a Chinese Espionage Campaign in Israel

Operational (OP) | Fusion (FS)

Strategic (ST) | Cyber Espionage (CE)

July 28, 2021 04:20:00 PM, 21-00016333, Version: 2

Executive Summary

By: Israel Research Team & U.S. Threat Intel Team

A version of this report will appear on the FireEye Threat Research Blog the week of July 26, 2021.

- This report details the post-compromise tradecraft and operational TTPs of a Chinese espionage group we track as UNC215. While UNC215's targets are located throughout the Middle East, Europe, Asia, and North America, this report focuses on intrusion activity primarily observed at Israeli entities.
- This report comes on the heels of the July 19, 2021, announcements by governments in North America, Europe, and Asia and intragovernmental organizations, such as the North Atlantic Treaty Organization (NATO), and the European Union,, condemning widespread cyber espionage conducted on behalf of the Chinese Government. These coordinated statements attributing sustained cyber espionage activities to the Chinese Government corroborate our long-standing reporting on Chinese threat actor targeting of private companies, governments, and various organizations around the world, and this blog shows yet another region where Chinese cyber espionage is active.

Threat Detail

In early 2019, Mandiant Threat Intelligence began identifying and responding to intrusions in the Middle East by Chinese espionage group UNC215, which we assess with moderate confidence is associated with APT27 (19-00010735). These intrusions exploited the Microsoft SharePoint vulnerability CVE-2019-0604 to install web shells and FOCUSFJORD payloads at targets in the Middle East and Central Asia.

In addition to data from Mandiant Incident Response and FireEye telemetry, we worked with Israeli defense agencies to review data from additional compromises of Israeli entities. This analysis showed multiple, concurrent operations against Israeli government institutions, IT providers, and telecommunications entities beginning in January 2019. During this time, UNC215 used new tactics, techniques, and procedures to hinder attribution and detection, maintain operational security (OPSEC), employ false flags, and leverage trusted relationships for lateral movement. We believe this adversary is still active in the region.

Attack Lifecycle

FIIP ENVIRONMENTS ORGANIZATION
sanaz.yashar@fireeye.com

Between 2019 and 2020, Mandiant responded to several incidents where Microsoft SharePoint vulnerability CVE-2019-0604 was used to deliver web shells, and then FOCUSFJORD payloads to select government and academic targets in the Middle East and Central Asia. During this time, we also detected numerous UNC215 phishing campaigns against government organizations in Kuwait and Turkey, diplomatic entities in Eastern Europe, and an online gambling organization in Southeast Asia (19-00019787, 19-00005220, 19-00021255, 19-00005968).

After gaining initial access, the operators conduct credential harvesting and extensive internal network reconnaissance. This includes running native Windows commands on compromised servers, executing ADFind on the Active Directory, and scanning the internal network with numerous publicly available tools and a non-public scanner we named WHEATSCAN. The operators made a consistent effort to delete these tools and remove any residual forensic artifacts from compromised systems.

In another incident response investigation, UNC215 pivoted to multiple OWA servers and installed web shells. In the following days, the operators interacted with these web shells from internal IP addresses, attempting to harvest credentials.

After identifying key systems within the target network, such as domain controllers and Exchange servers, UNC215 moved laterally and deployed their signature malware FOCUSFJORD. UNC215 often uses FOCUSFJORD for the initial stages of an intrusion, and then later deploys HYPERBRO, which has more information collection capabilities such as screen capture and keylogging. While UNC215 heavily relies on the custom tools FOCUSFJORD and HYPERBRO, Chinese espionage groups often have resource sharing relationships with other groups, and we do not have enough information to determine if these tools are developed and used exclusively by UNC215.

FIIP ENVIRONMENTS ORGANIZATION
sanaz.yashar@fireeye.com

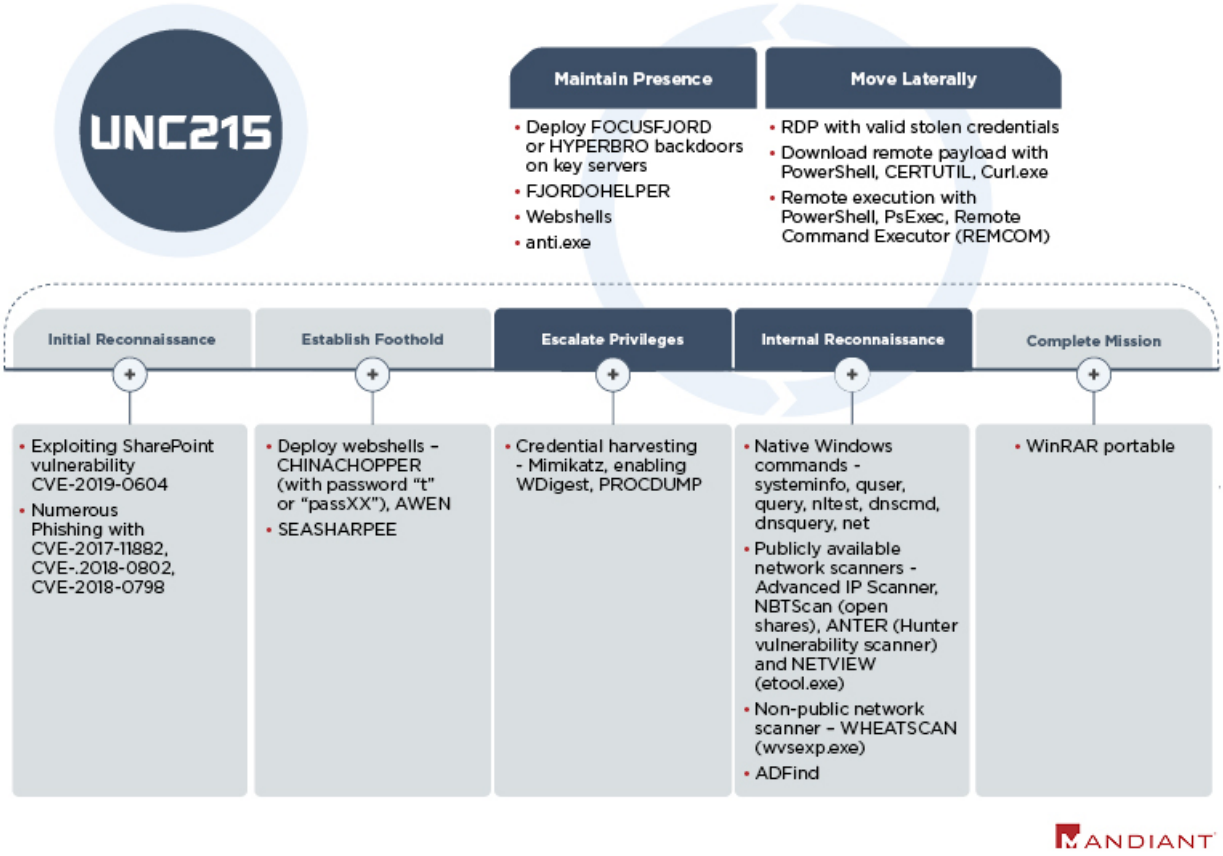

Figure 1: Attack lifecycle

Tradecraft and Operational Security

We identified numerous examples of efforts by UNC215 to foil network defenders by minimizing forensic evidence left on compromised hosts, exploiting relationships with trusted third parties, continuously improving the FOCUSFJORD backdoor, concealing command and control (C&C) infrastructure, and incorporating false flags.

Reducing Forensic Evidence on Disk

UNC215 consistently cleaned up evidence of their intrusion after gaining access to a system. This type of action can make it more difficult for incident responders to reconstruct what happened during a compromise.

- The operators deleted tools used for credential harvesting and internal reconnaissance including a custom scanner dubbed WHEATSCAN after use.
- The first FOCUSFJORD payload delivered to a system contains a blob that includes C&C and other configuration data. On initial execution, FOCUSFJORD writes its encrypted C&C configuration into the system's registry, sets up a persistence mechanism and then rewrites itself on disk without the embedded configuration and with limited functionality to only read configuration data. This process enables the operators to obfuscate the configured C&C servers from automated sandbox runs or disclosure in public file scanning services.
- A newly identified utility dubbed FJORDOHELPER can update FOCUSFJORD configurations and completely remove FOCUSFJORD from the system. The tool can be deployed and executed remotely to delete any remaining FOCUSFJORD forensic

evidence, including files on disk, configuration data encrypted in the registry, and related services and registry keys used for persistence.

Exploiting Trust Relationships

UNC215 leveraged trusted third parties in a 2019 operation targeting an Israeli government network. As illustrated in Figure 2, the operators were able to access their primary target via RDP connections from a trusted third party using stolen credentials and used this access to deploy and remotely execute FOCUSFJORD on their primary target.

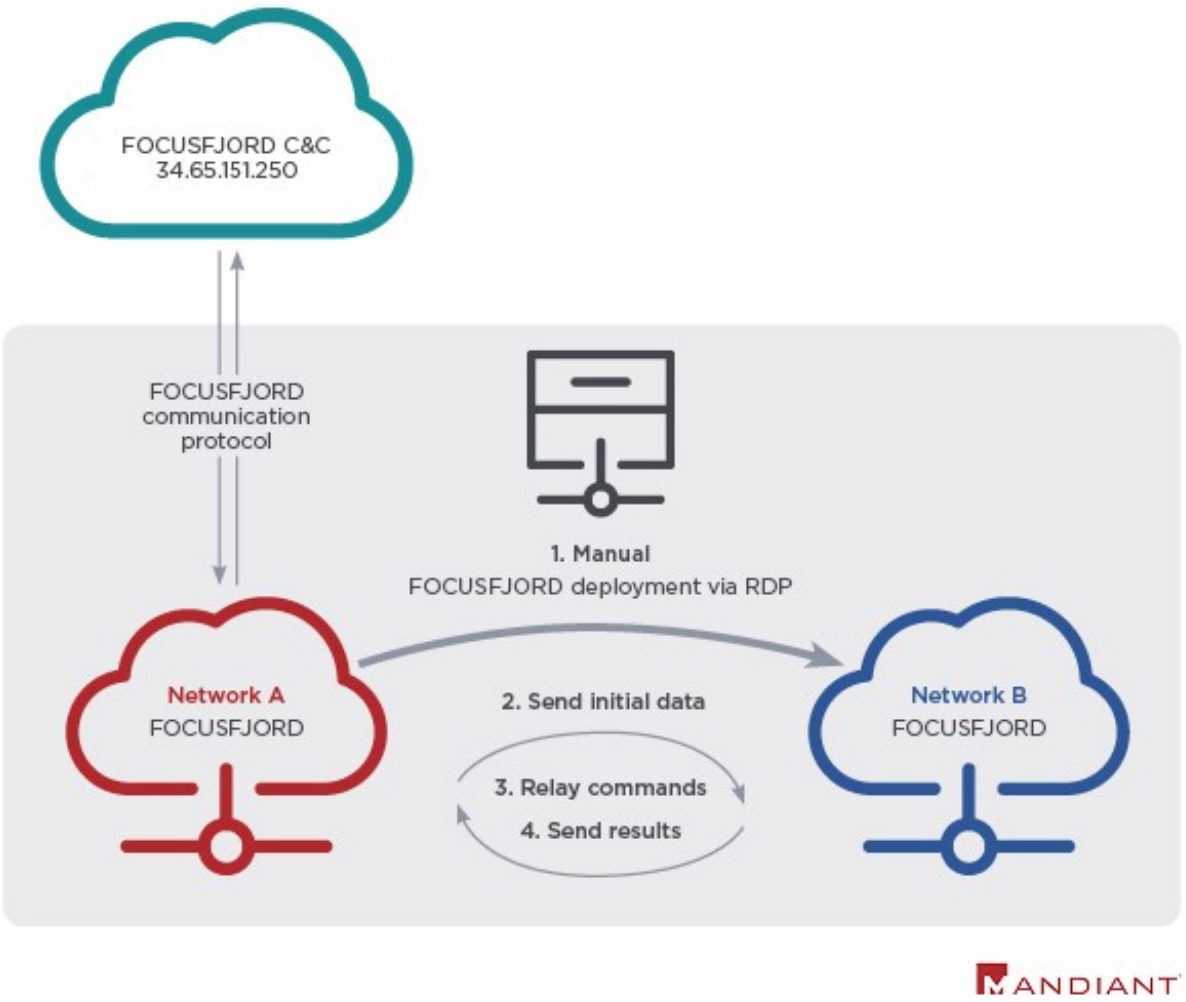

Figure 2: Two FOCUSFJORD samples configured to proxy C&C traffic

Concealing C&C Infrastructure

UNC215 made technical modifications to their tools to limit outbound network traffic and used other victim networks to proxy their C&C instructions, likely to minimize the risk of detection and blend in with normal network traffic. We examined HYPERBRO and FOCUSFJORD samples capable of acting as proxies to relay communications to their C&C servers.

- HYPERBRO samples MD5: 0ec4d0a477ba21bda9a96d8f360a6848 and MD5: 04dece2662f648f619d9c0377a7ba7c0 have embedded configurations of internal IP addresses (192[.]168[.]1[.]237 and 192[.]168[.]4[.]26 respectively) as C&C servers. If

they receive a command with an IP address and port, they will connect and relay the command.

- FOCUSFJORD sample MD5: e3e1b386cdc5f4bb2ba419eb69b1b921 has an internal IP address, 192[.]168[.]4[.]197, configured as its C&C. This sample was extracted from MD5: c25e8e4a2d5314ea55afd09845b3e886, which was submitted to a public malware repository in December 2017.

While hunting for FOCUSFJORD samples, we found a sample MD5: 625dd9048e3289f19670896cf5bca7d8 that shares code with FOCUSFJORD. However, analysis indicates that it only contains functions to relay communications between another FOCUSFJORD instance and a C&C server (Figure 2, Network A). We suspect this type of malware was used in the above-mentioned operation. The actors stripped out unnecessary FOCUSFJORD capabilities, possibly to reduce the likelihood it would be detected by security controls. Figure 3 below contains the data structure as it is being sent from a FOCUSFJORD sample configured to communicate with another FOCUSFJORD victim.

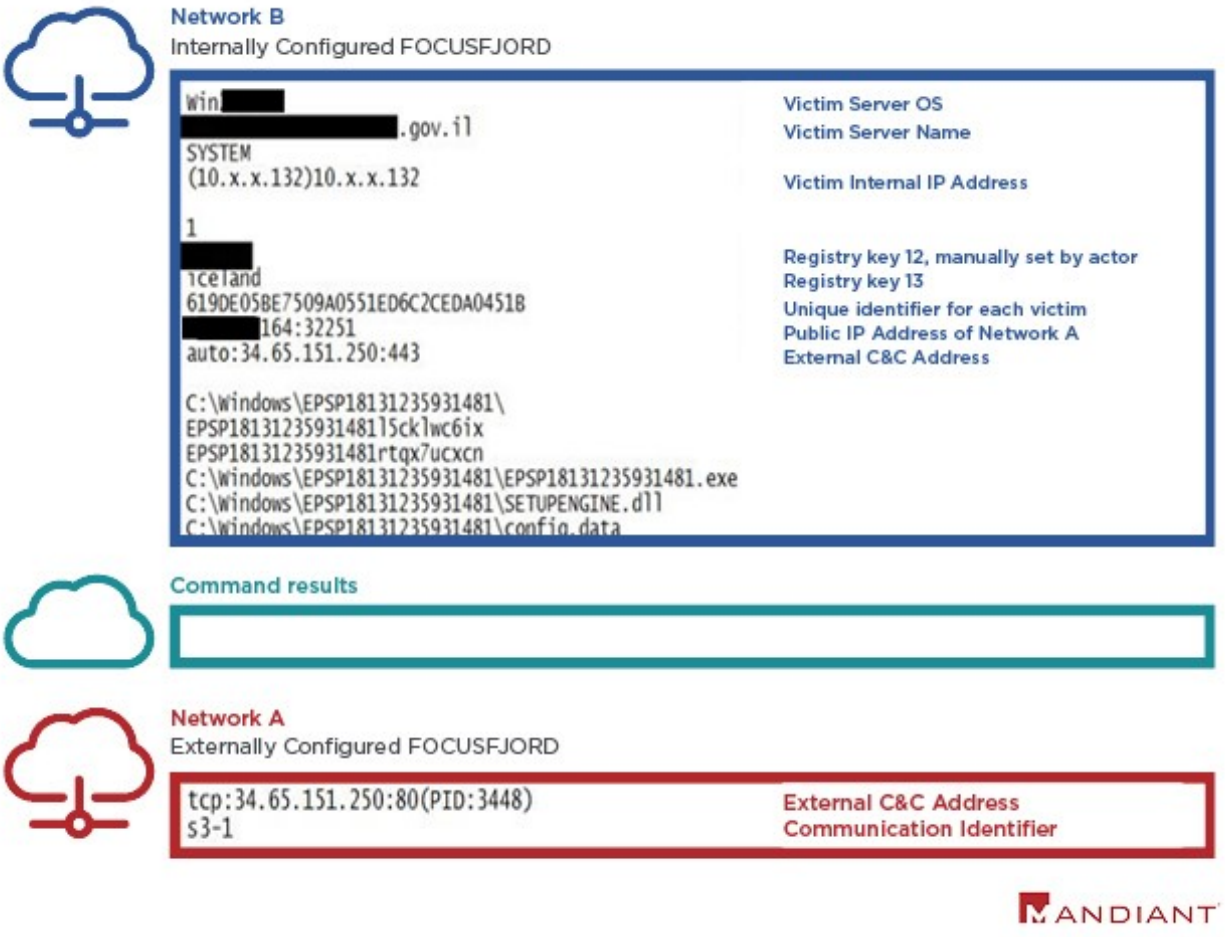

Figure 3: Decrypted data sent from the internally configured FOCUSFJORD

FOCUSFJORD Changes

We have observed numerous variants of the FOCUSFJORD malware family since 2017. The authors have added new communications protocols, an updated loading mechanism, and expanded the number of supported configurations in newer versions. Version numbers indicate that the malware undergoes frequent changes and maybe supported by a team of developers. Many of these variants contain or remove functionality depending on the

operator's unique requirements at the time, which may suggest that multiple operators have access to the source code or a builder, or that a close relationship exists between the developers and operators.

FOCUSFJORD samples can be configured with up to 13 unique registry values which allow operators to control and organize compromised hosts. In addition to specifying details related to the loading and persistence mechanisms and C&C communications, there are two keys that allow the operator to add additional context about the victim:

- Registry key 12 is the "group" name. When a new FOCUSFJORD sample is first executed and writes its configuration to registry, this value is set to "default" and is later manually changed by the actor, usually to the victim's domain name or organization name.
- Registry key 13 could be interpreted as the "console" name, although we do not fully understand how the identifier is used by the operators. We have observed the values "galway," "iceland," "helen," and "idapro."

It is unclear how or if UNC215 uses these configuration parameters to organize and track large numbers of compromised hosts. We observed different console values within the same network, identical console values using different C&C addresses, and identical console values targeting different countries. Some FOCUSFJORD samples from 2018 and 2020 use the same console values despite the significant gap in time (Table 1).

- The NCC Group discussed these configurations in a 2018 report and released a decoding tool.
- TrendMicro noted changes to supported configurations in FOCUSFJORD, dubbed SysUpdate, in their 2020 and 2021 reports following public disclosures. This suggests that operators using FOCUSFJORD are sensitive to security vendor reports and will update the code to avoid detection and exposure.

Registry Key 13	FOCUSFJORD MD5 Hash	Related C&C	Suspected Target
helen	3d95e1c94bd528909308b198f3d47620	139[.]59[.]81[.]253	Israel
helen	f335b241652cb7f7e736202f14eb48e9	139[.]59[.]81[.]253	Israel
helen	a0b2193362152053671dbe5033771758	139[.]59[.]81[.]253	Israel
helen	6a9a4da3f7b2075984f79f67e4eb2f28	139[.]59[.]81[.]253	Kazakhstan
helen	a19370b97fe64ca6a0c202524af35a30	159[.]89[.]168[.]83	Iran
helen	3c1981991cce3b329902288bb2354728	103[.]59[.]144[.]183	Unknown
iceland	26d079e3afb08af0ac4c6d92fd221e71	178[.]79[.]177[.]69	UAE
iceland	19c46d01685c463f21ef200e81cb1cf1	138[.]68[.]154[.]133	UAE
iceland	28ce8dbdd2b7dfd123cebbfff263882c	138[.]68[.]154[.]133	Unknown
iceland	a78c53351e23d3f84267e67bbca6cf07	206[.]189[.]123[.]156	Israel (Gov), UAE
iceland	a78c53351e23d3f84267e67bbca6cf07	206[.]189[.]123[.]156	Israel (IT)
idapro	a78c53351e23d3f84267e67bbca6cf07	206[.]189[.]123[.]156	Israel (IT)
galway	04c51909fc65304d907b7cb6c92572cd	159[.]65[.]80[.]157	Unknown
galway	0e061265c0b5998088443628c03188f0	159[.]65[.]80[.]157	Unknown

galway	09ffc31a432f646ebcec59d32f286317	159[.]65[.]80[.]157	Unknown
galway	6ca8993b341bd90a730faef1fb73958b	128[.]199[.]44[.]86	Unknown
helen	Unknown	46[.]101[.]255[.]16	Iran
helen	Unknown	178[.]79[.]143[.]78	Iran
idapro	Unknown	138[.]68[.]154[.]133	Iran

Table 1: FOCUSFJORD comparison

False Flags

Artifacts in UNC215 campaigns often contain foreign language strings that do not match the country being targeted and may be intended to mislead an analyst examining the malware. Additionally, on at least three occasions, UNC215 employed a custom tool associated with Iranian actors whose source code was leaked.

- In several cases, we identified FOCUSFJORD samples with registry key names in regional languages. The registry key names are hardcoded into every FOCUSFJORD sample, as the malware needs to read and decrypt those registry key values for proper execution.
  - FOCUSFJORD samples (MD5: d13311df4e48a47706b4352995d67ab0 and MD5: 26d079e3afb08af0ac4c6d92fd221e71) observed on Israeli and UAE networks, and a memory dump (MD5: d875858dbd84b420a2027ef5d6e3a512) submitted to a public malware repository by a likely Uzbekistan financial organization are configured with registry keys in Farsi. Linguistic analysis suggests that these terms were auto translated as they are not commonly used by native Farsi speakers.
  - Another FOCUSFJORD sample uploaded from Uzbekistan (MD5: ac431261b8852286d99673fddba38a50) contains a configuration with registry key names in Hindi. Notably, this variant also contains an error message string in Arabic ('ضائع' – which translates to "lost" or "missing").
- In April 2019, UNC215 deployed the SEASHARPEE web shell against financial and high-tech organizations in the Middle East and Asia. The SEASHARPEE web shell was developed and used by Iranian APT actors until the code was leaked online in the telegram channel Lab Dookhtegan a few weeks earlier in March 2019 (19-00005968, 19-00006730).
- Around this time, the Turkish-language file Sosyal Güvenlik Reformu-Not-3[.]doc "Social Security Reform - Note - 3[.]doc" (MD5: 6930bd66a11e30dee1ef4f57287b1318) was distributed to Turkish government entities via targeted email based on data from an open-source malware repository. The document contains "C:\Users\Iran" paths that were likely included to obfuscate the source of the activity.

The use of Farsi strings, filepaths containing /Iran/, and web shells publicly associated with Iranian APT groups may have been intended to mislead analysts and suggest an attribution to Iran. Notably, in 2019 the government of Iran accused APT27 of attacking its government networks and released a detection and removal tool for HYPERBRO malware.

Tradecraft Mistakes

While UNC215 prioritizes evading detection within a compromised network, Mandiant identified several examples of code, C&C infrastructure, and certificate reuse indicating that UNC215 operators are less concerned about defenders' ability to track and detect UNC215 activity.

- In several instances, UNC215 used the same exact file against multiple victims and frequently shared infrastructure across victims. This lack of attention to detail a is not uncommon and may suggest that on occasion, UNC215's rapid operational tempo leads to mistakes.
  - The HYPERBRO loader (MD5: 2bdc1fc71bf3e2e4c6cf51b975607fea) was used against an Israeli high-tech company, a victim in the southeast Asian media, and entertainment sector and targeted the UAE.
  - HYPERBRO shellcode (MD5: 09396e181db546debb87632e439beb32) was used in an operation targeting an Israeli high-tech company in December 2019 and in another operation targeting a different Israeli high-tech company. Its embedded C&C 85[.]204[.]74[.]143 was also used in another HYPERBRO sample (MD5: ad72e6cf7bfa37a2bae835c5d5d1e96f), which was submitted to a malware repository in September 2019.
  - FOCUSFJORD loader (MD5: b3b9ac7a454bba9994001f0a694b1916) was used in an operation targeting Israeli government entities, and in another operation targeting an Israeli IT company. This loader was used to load FOCUSFJORD shellcode (MD5: a78c53351e23d3f84267e67bbca6cf07) in these operations and it was distributed to an unknown UAE entity in June 2019.
  - WHEATSCAN (MD5: f1f2b14114e1788fae4ff7d0e8574a93) was used in two different operations targeting Israeli government entities within a short timeframe. We found a similar sample (MD5: 44606907982b063eccb8607d31265d09) with the same filename "wvsexp[.]exe" on a malware repository, submitted from Iran in December 2019.
- We identified multiple FOCUSFJORD samples configured to use the same C&C servers across multiple victims. Additionally, C&C IP 85[.]204[.]74[.]143 was identified as the C&C for three different HYPERBRO samples (MD5: 09396e181db546debb87632e439beb32, MD5: ad72e6cf7bfa37a2bae835c5d5d1e96f, MD5: 278ef49ae186beb9f1f5676f1a1cd2f4).
- C&C servers used by UNC215 frequently reuse the same SSL certificate as described in Team Cymru's research in 2020.

On one network, between April 2019 and April 2020, an operator repeatedly and infrequently revisited a compromised network whenever an Endpoint Detection and Response (EDR) tool detected or quarantined tools like HYPERBRO and Mimikatz. After several months of repeated detections, UNC215 deployed an updated version of HYPERBRO and a tool called "anti[.]exe" to stop Windows Update service and terminates EDR and Antivirus related services.

Attribution

Mandiant attributes this campaign to Chinese espionage operators which we tracked as UNC215. We have moderate confidence that UNC215 is associated with APT27, a Chinese espionage operation that has been suspected of targeting organizations around the world

since at least 2011. UNC215 has compromised organizations in the government, technology, telecommunications, defense, finance, entertainment, and healthcare sectors. The group targets data and organizations which are of great interest to Beijing's financial, diplomatic, and strategic objectives.

Outlook and Implications

The activity detailed above demonstrates China's consistent strategic interest in the Middle East. This cyber espionage activity is happening against the backdrop of China's multi-billion-dollar investments related to the Belt and Road Initiative (BRI) and its interest in Israeli's robust technology sector.

- Chinese companies have invested billions of dollars into Israeli technology startups, partnering or acquiring companies in strategic industries like semi-conductors and artificial intelligence.
- As China's BRI moves westward, its most important construction projects in Israel are the railway between Eilat and Ashdod, a private port at Ashdod, and the port of Haifa.

China has conducted numerous intrusion campaigns along the BRI route to monitor potential obstructions—political, economic, and security—and we anticipate that UNC215 will continue targeting governments and organizations involved in these critical infrastructure projects in Israel and the broader Middle East in the near and mid-term.

MITRE ATT&CK Techniques

ID	Technique
T1003.001	OS Credential Dumping: LSASS Memory
T1007	System Service Discovery
T1010	Application Window Discovery
T1012	Query Registry
T1016	System Network Configuration Discovery
T1021.001	Remote Services: Remote Desktop Protocol
T1027	Obfuscated Files or Information
T1033	System Owner/User Discovery
T1055	Process Injection
T1055.003	Process Injection: Thread Execution Hijacking
T1055.012	Process Injection: Process Hollowing
T1056.001	Input Capture: Keylogging
T1057	Process Discovery
T1059.001	Command and Scripting Interpreter: PowerShell
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1070.004	Indicator Removal on Host: File Deletion
T1070.006	Indicator Removal on Host: Timestomp
T1071.001	Application Layer Protocol: Web Protocols
T1078	Valid Accounts
T1082	System Information Discovery

T1083	File and Directory Discovery
T1087	Account Discovery
T1090	Proxy
T1095	Non-Application Layer Protocol
T1098	Account Manipulation
T1105	Ingress Tool Transfer
T1112	Modify Registry
T1113	Screen Capture
T1115	Clipboard Data
T1133	External Remote Services
T1134	Access Token Manipulation
T1140	Deobfuscate/Decode Files or Information
T1190	Exploit Public-Facing Application
T1199	Trusted Relationship
T1202	Indirect Command Execution
T1213	Data from Information Repositories
T1482	Domain Trust Discovery
T1489	Service Stop
T1497	Virtualization/Sandbox Evasion
T1497.001	Virtualization/Sandbox Evasion: System Checks
T1505.003	Server Software Component: Web Shell
T1518	Software Discovery
T1543.003	Create or Modify System Process: Windows Service
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1553.002	Subvert Trust Controls: Code Signing
T1559.002	Inter-Process Communication: Dynamic Data Exchange
T1560	Archive Collected Data
T1564.003	Hide Artifacts: Hidden Window
T1569.002	System Services: Service Execution
T1573.002	Encrypted Channel: Asymmetric Cryptography
T1574.002	Hijack Execution Flow: DLL Side-Loading
T1583.003	Acquire Infrastructure: Virtual Private Server
T1588.003	Obtain Capabilities: Code Signing Certificates
T1608.003	Stage Capabilities: Install Digital Certificate

Table 2: MITRE ATT&CK techniques

Indicators of Compromise

Type	Value	Description
IP	185[.]12[.]45[.]134	HYPERBRO C&C
IP	85[.]204[.]74[.]143	HYPERBRO C&C
IP	103[.]79[.]78[.]48	HYPERBRO C&C
IP	89[.]35[.]178[.]105	HYPERBRO C&C
IP	47[.]75[.]49[.]32	HYPERBRO C&C

IP	139[.]59[.]81[.]253	FOCUSFJORD C&C
IP	206[.]189[.]123[.]156	FOCUSFJORD C&C
IP	66[.]42[.]62[.]250	FOCUSFJORD C&C
IP	178[.]128[.]165[.]84	FOCUSFJORD C&C
IP	34[.]93[.]247[.]126	FOCUSFJORD C&C
IP	34[.]65[.]151[.]250	FOCUSFJORD C&C
IP	159[.]89[.]168[.]83	FOCUSFJORD C&C
IP	103[.]59[.]144[.]183	FOCUSFJORD C&C
IP	178[.]79[.]177[.]69	FOCUSFJORD C&C
IP	159[.]65[.]80[.]157	FOCUSFJORD C&C
IP	128[.]199[.]44[.]86	FOCUSFJORD C&C
IP	141[.]164[.]52[.]232	FOCUSFJORD C&C

Table 3: Indicators of compromise

Please rate this product by taking a short four question survey

First Version Publish Date

July 28, 2021 02:55:00 PM

Threat Intelligence Tags

Affected Industry

- Government - National
- Technology
- Telecommunications
- Education

Target Geography

- Israel

Intended Effect

- Political Advantage
- Competitive Advantage in Business or Economic Advantage

Motivation

- Military/Security/Diplomatic

Source Geography

- China

Tactics, Techniques And Procedures(TTPs)

- Communications
- Malware Propagation and Deployment

- Network Reconnaissance
- Social Engineering

Actor

- UNC215

Malware Family

- WHEATSCAN
- HYPERBRO
- FOCUSFJORD
- SFXRAR
- SILKWRAP

Technical Indicators & Warnings

IP:	159[.]89[.]168[.]83
Identifier:	Related
Network Type:	network
IP:	185[.]161[.]210[.]97
Identifier:	Related
Network Type:	network
IP:	139[.]59[.]81[.]253
Identifier:	Related
Network Type:	network
IP:	34[.]65[.]151[.]250
Identifier:	Related
Network Type:	network
IP:	103[.]59[.]144[.]183
Identifier:	Related
Network Type:	network
IP:	141[.]164[.]52[.]232
Identifier:	Related
Network Type:	network
IP:	206[.]189[.]123[.]156
Identifier:	Related
Network Type:	network
IP:	34[.]93[.]247[.]126
Identifier:	Related
Network Type:	network

IP:	138[.]68[.]154[.]133
Identifier:	Related
Network Type:	network
IP:	85[.]204[.]74[.]143
Identifier:	Related
Network Type:	network
IP:	78[.]141[.]219[.]106
Identifier:	Related
Network Type:	network
IP:	46[.]101[.]255[.]16
Identifier:	Related
Network Type:	network
IP:	47[.]75[.]49[.]32
Identifier:	Related
Network Type:	network
IP:	95[.]179[.]189[.]33
Identifier:	Related
Network Type:	network
IP:	185[.]12[.]45[.]134
Identifier:	Related
Network Type:	network
IP:	66[.]42[.]62[.]250
Identifier:	Related
Network Type:	network
IP:	128[.]199[.]44[.]86
Identifier:	Related
Network Type:	network
IP:	178[.]79[.]177[.]69
Identifier:	Related
Network Type:	network
IP:	34[.]90[.]207[.]23
Identifier:	Related
Network Type:	network
IP:	89[.]35[.]178[.]105
Identifier:	Related
Network Type:	network
IP:	178[.]128[.]165[.]84

Identifier:	Related
Network Type:	network
IP:	178[.]79[.]143[.]78
Identifier:	Related
Network Type:	network
IP:	159[.]65[.]80[.]157
Identifier:	Related
Network Type:	network
IP:	103[.]79[.]78[.]48
Identifier:	Related
Network Type:	network
SHA1:	d3da63fcbb591c7f48e3682e38137f8009d6ffa4
File Name:	gvg36a467c6hkea
Identifier:	Attacker
File Size:	260473
SHA256:	fe778a41e32ea4a36fca2aea8ffb5d8c02de38e84c6b158077f9c77b4ea1c4d8
Type:	application/octet-stream
MD5:	3d95e1c94bd528909308b198f3d47620
Malware Family:	FOCUSFJORD
SHA1:	4617c9f7781d584996875fe0bf5ad198bcf392a5
File Name:	ef51b08234488b6cb51eb949dff5b7421e9a040f73c10a40d5320dac561d944f
Identifier:	Related
File Size:	400384
SHA256:	ef51b08234488b6cb51eb949dff5b7421e9a040f73c10a40d5320dac561d944f
Type:	application/x-dosexec
MD5:	625dd9048e3289f19670896cf5bca7d8
SHA1:	7ced00732dec8a07e0cdb0f9e3b7e0606e5031be
File Name:	wvsexp[.]exe
Identifier:	Attacker
File Size:	218624
SHA256:	90daf97ebc088c51d297dba6c0b6dc40f96e8ab2ed3604ba8e9ddbd97a52fb99
Type:	application/x-dosexec
MD5:	44606907982b063eccb8607d31265d09
Malware Family:	WHEATSCAN
SHA1:	187907ba32af48d49ef7a2a41734d1349408a17a
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	737280
SHA256:	53078657e4e83d703f1f3b41f87dbea20c1ae78d58826ec3223864370669ae8d

Type:	application/x-dosexec
MD5:	d13311df4e48a47706b4352995d67ab0
Malware Family:	FOCUSFJORD
SHA1:	f9b1202803f0301c09c66b28354ede3e7eab2d8b
File Name:	payload
Identifier:	Attacker
File Size:	164864
SHA256:	9e1a44fb1713150950834777ecc1c39efda905a0c0bdeafce7410934cf08bd1c
Type:	application/x-dosexec
MD5:	278ef49ae186beb9f1f5676f1a1cd2f4
Malware Family:	HYPERBRO
SHA1:	725e1300954e29a748499f730065e55960130547
File Name:	thumb[.]dat
Identifier:	Attacker
File Size:	110557
SHA256:	601a02b81e3bd134c2cf681ac03d696b446e10bf267b11b91517db1b233fec74
Type:	application/octet-stream
MD5:	ad72e6cf7bfa37a2bae835c5d5d1e96f
Malware Family:	SILKWRAP
SHA1:	27522f3c8675b024f5aa9e19c3abf7b3563deca0
File Name:	payload
Identifier:	Attacker
File Size:	220672
SHA256:	a6556e9d2a41b2b46cb48bfef51b1f27d823f4467b16c53a6a744f0b02d16d9e
Type:	application/x-dosexec
MD5:	0e061265c0b5998088443628c03188f0
Malware Family:	FOCUSFJORD
SHA1:	3945bc92e49a5d572c9202f0bd859dd2e9ec4168
File Name:	emm_pand_decryp[.]bin
Identifier:	Attacker
SHA256:	81b7414d01aab21963710da1eca2634b6c1d87eb2aecafb30f915901867244f9
Type:	application/x-dosexec
MD5:	28ce8dbdd2b7dfd123cebbfff263882c
Malware Family:	FOCUSFJORD
SHA1:	6792886b0527d80b337b499e715a252b2775a0d6
File Name:	payload
Identifier:	Related
File Size:	441344
SHA256:	67c789071b25b170bbd93dc768f75d89092ff107a9f2a2be4ce739e7086fd4d2
Type:	application/x-dosexec
MD5:	26d079e3afb08af0ac4c6d92fd221e71

SHA1:	d04642c5ab7b5edab85fda46b67f19368af0d381
File Name:	SETUPENGINE[.]dll
Identifier:	Attacker
File Size:	34816
SHA256:	aed87f0c0fa5af4cd28349c80e8a6d285a4b92fd000053ba3ee305eed934435e
Type:	application/x-dosexec
MD5:	b3b9ac7a454bba9994001f0a694b1916
Malware Family:	FOCUSFJORD

SHA1:	ddee9282bab537136f563f3c93856e5793ab9e5a
File Name:	Sosyal Güvenlik Reformu-Not-3[.]doc
Identifier:	Attacker
File Size:	291090
SHA256:	3e04eb55095ad6a45905564d91f2ab6500e07afcdf9d6c710d6166d4eef28185
Type:	text/rtf
MD5:	6930bd66a11e30dee1ef4f57287b1318
Malware Family:	HYPERBRO

SHA1:	d68429a7dfd21400000d511e998ec95c64d424db
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	220672
SHA256:	3390928b0d5faaada9665f2aac5a4c6be787267615a54b73bb9c855894ef9572
Type:	application/x-dosexec
MD5:	f1f2b14114e1788fae4ff7d0e8574a93
Malware Family:	WHEATSCAN

SHA1:	b1300b57f928820dc794fafb22de94279fac49ae
File Name:	mpsvc[.]dll
Identifier:	Attacker
SHA256:	6655c84e064f744e99fc4d7e50487239604df5f97996eaa8507df7744a8b4de3
Type:	application/x-dosexec
MD5:	2bdc1fc71bf3e2e4c6cf51b975607fea
Malware Family:	HYPERBRO

SHA1:	6efcbb15969b4a017812522ba183ab9702050145
File Name:	payload
Identifier:	Attacker
File Size:	219648
SHA256:	f430ce22ffa258a09b5a555549918c311f014f264e451c0c539b8ec019726c2d
Type:	application/x-dosexec
MD5:	09ffc31a432f646ebcec59d32f286317
Malware Family:	FOCUSFJORD

SHA1:	765cebd9e46f5c511611a09d5ee78b2daba16a9e

File Name:	gvg36[.]bin
Identifier:	Attacker
File Size:	276521
SHA256:	e05e853cca1a8e9c8b1674f59c27b562887742f3110499f8ff38d0d287f0e7de
Type:	application/octet-stream
MD5:	ac431261b8852286d99673fddba38a50
Malware Family:	SILKWRAP
SHA1:	e100096e52df7f7616faae59fa47467ed89f47d7
File Name:	file
Identifier:	Attacker
File Size:	126976
SHA256:	325d272762877eed35526408410c433f6c80fc0c019bad5b740a4d548e67288f
Type:	application/x-dosexec
MD5:	0ec4d0a477ba21bda9a96d8f360a6848
Malware Family:	HYPERBRO
SHA1:	cb66bcd73bd40d902bc05e74dcf59dc3c6f09861
File Name:	gvg36a467c6hkea
Identifier:	Attacker
File Size:	260475
SHA256:	7a188b28720a68c0dcfb8bdb0793aca55b1ca06d15de22c836e1a7aa43314cb2
Type:	application/octet-stream
MD5:	f335b241652cb7f7e736202f14eb48e9
Malware Family:	FOCUSFJORD
SHA1:	e8cf3522b68a51b2aabcfc6f98b39da15a23da1d
File Name:	76bc063f8f348a202f92faac0c36f1a0a122f9b3568342abcd97651be7adec08
Identifier:	Attacker
File Size:	310734
SHA256:	76bc063f8f348a202f92faac0c36f1a0a122f9b3568342abcd97651be7adec08
Type:	application/x-dosexec
MD5:	c25e8e4a2d5314ea55afd09845b3e886
Malware Family:	SFXRAR
SHA1:	ac4a264a76ba22e21876f7233cbdbe3e89b6fe9d
File Name:	20200131-ZZ-Unknown/Related/19c46d01685c463f21ef200e81cb1cf1
Identifier:	Attacker
SHA256:	3e21e7ea119a7d461c3e47f50164451f73d5237f24208432f50e025e1760d428
Type:	application/octet-stream
MD5:	19c46d01685c463f21ef200e81cb1cf1
Malware Family:	FOCUSFJORD
SHA1:	d2ebd63b9038e7d77b8773bdba309beb7c46c593
File Name:	3ffb8343387bd208a59811b632007a357933a5587eb7f7e10d234b2bc1643625

Identifier:	Attacker
File Size:	81920
SHA256:	3ffb8343387bd208a59811b632007a357933a5587eb7f7e10d234b2bc1643625
Type:	application/x-dosexec
MD5:	04dece2662f648f619d9c0377a7ba7c0
Malware Family:	HYPERBRO
SHA1:	701e9c1657e2dc538546def3c50eb37ed32732d9
File Name:	UNAVAILABLE
Identifier:	Attacker
File Size:	58211
SHA256:	9489f68b4000c096027186568783c19bb52043493006c334b601ae65c86c5f03
Type:	application/octet-stream
MD5:	09396e181db546debb87632e439beb32
Malware Family:	HYPERBRO
SHA1:	c0bc728e2ecc52e27a5941a8675b964a0a925d0a
File Name:	wtsapi32[.]hlp
Identifier:	Attacker
File Size:	260505
SHA256:	6c10515df8f61b2aa478cbd5573e93ba90ca38724b4f125212debd0e3c25b76d
Type:	application/octet-stream
MD5:	a19370b97fe64ca6a0c202524af35a30
Malware Family:	FOCUSFJORD
SHA1:	f46e0f58298a65b4552527fc374b826960a09e1a
File Name:	cfgwiz_dump_370000[.]dll
Identifier:	Attacker
File Size:	397824
SHA256:	0ac3c9e92c0d6494b762d4035f667dc817a48e45a581d184481e0b87e071304c
Type:	application/x-dosexec
MD5:	a0b2193362152053671dbe5033771758
Malware Family:	FOCUSFJORD
SHA1:	b1d9f69f6a2f771fee8e16323d0825657552273e
File Name:	sys[.]bin[.]url
Identifier:	Attacker
File Size:	76089
SHA256:	b0230ffd936b50176b3f12a826d783dc2385bfcd2b612e84f47d98824d1f42ef
Type:	application/octet-stream
MD5:	e3e1b386cdc5f4bb2ba419eb69b1b921
Malware Family:	FOCUSFJORD
SHA1:	c750c12b22fb56092b6e93289e787bf4ed11ecc3
File Name:	gvg36a467c6hkea
Identifier:	Attacker

File Size:	260466
SHA256:	ab6998352fc0d745af94f02e42f8c3f061a99179fce2c890760f293f9744d1e8
Type:	application/octet-stream
MD5:	6a9a4da3f7b2075984f79f67e4eb2f28
Malware Family:	FOCUSFJORD
SHA1:	1a31927edc1f014636131ab2f5a937baba625707
File Name:	sys[.]bin[.]url
Identifier:	Attacker
File Size:	148364
SHA256:	3b33f4630c2debf5eca4f758c194870238cf765e7f9b5733ab096ea0c705dbe4
Type:	application/octet-stream
MD5:	3c1981991cce3b329902288bb2354728
Malware Family:	SILKWRAP
SHA1:	e75825e1ed327a05ce1bbaf6fd7d972a1a6f1d38
File Name:	setupengine[.]hlp
Identifier:	Attacker
File Size:	257213
SHA256:	7d1fb4c37c5148691c97fc6122692260b804ae33ba6a7a18c55027fb737b0752
Type:	application/octet-stream
MD5:	a78c53351e23d3f84267e67bbca6cf07
Malware Family:	FOCUSFJORD
SHA1:	ce7d9b0a88df7b80ffa4da093536593dae2fdeb7
File Name:	dllhost[.]dmp
Identifier:	Related
File Size:	48718455
SHA256:	b645ff7ca1bce2a9449bcf7378895022170ec8adba62ccf528e453667da2210a
Type:	application/octet-stream
MD5:	d875858dbd84b420a2027ef5d6e3a512
SHA1:	290ad4fe5b1a7fda521378ac379367e20d438c8c
File Name:	c69_loader[.]bin
Identifier:	Attacker
SHA256:	caa02607d30935f5ea38b0a3073372e9ca37efc0d44df945adb191c745e389af
Type:	application/x-dosexec
MD5:	6ca8993b341bd90a730faef1fb73958b
Malware Family:	FOCUSFJORD
SHA1:	c23cab19e10ebbe60e3915f2d11565b84fcc1625
File Name:	0d98_c30000[.]bin
Identifier:	Attacker
SHA256:	bb8237a721b151443234b853e8720cff7350913a26d96abe97fe6b5946885068
Type:	application/x-dosexec

MD5:	04c51909fc65304d907b7cb6c92572cd
Malware Family:	FOCUSFJORD

Common Vulnerabilities and Exposures

CVE ID:	CVE-2019-0604(NVD Description)External Link

Version Information

Version:1.0, July 28, 2021 02:55:00 PM
UNC215: Spotlight on a Chinese Espionage Campaign in Israel

Version:2.0, July 28, 2021 04:20:00 PM
UNC215: Spotlight on a Chinese Espionage Campaign in Israel

5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

For more information please visit: https://intelligence.fireeye.com/reports/21-00016333