UNC215: Spotlight on a Chinese Espionage Campaign in Israel

mandiant.com/resources/unc215-chinese-espionage-campaign-in-israel

Breadcrumb

Threat Research

Israel Research Team, U.S. Threat Intel Team

Aug 10, 2021

13 mins read

Threat Research

Uncategorized Groups (UNC Groups)

This blog post details the post-compromise tradecraft and operational tactics, techniques, and procedures (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 post shows yet another region where Chinese cyber espionage is active.

Threat Detail

In early 2019, Mandiant began identifying and responding to intrusions in the Middle East by Chinese espionage group UNC215. 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. There are targeting and high level technique overlaps with between UNC215 and APT27, but we do not have sufficient evidence to say that the same actor is responsible for both sets of activity. APT27 has not been seen since 2015, and UNC215 is targeting many of the regions that APT27 previously focused on; however, we have not seen direct connection or shared tools, so we are only able to assess this link with low confidence.

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 TTPs to hinder attribution and detection, maintain operational security, employ false flags, and leverage trusted relationships for lateral movement. We believe this adversary is still active in the region.

Attack Lifecycle

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.

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.

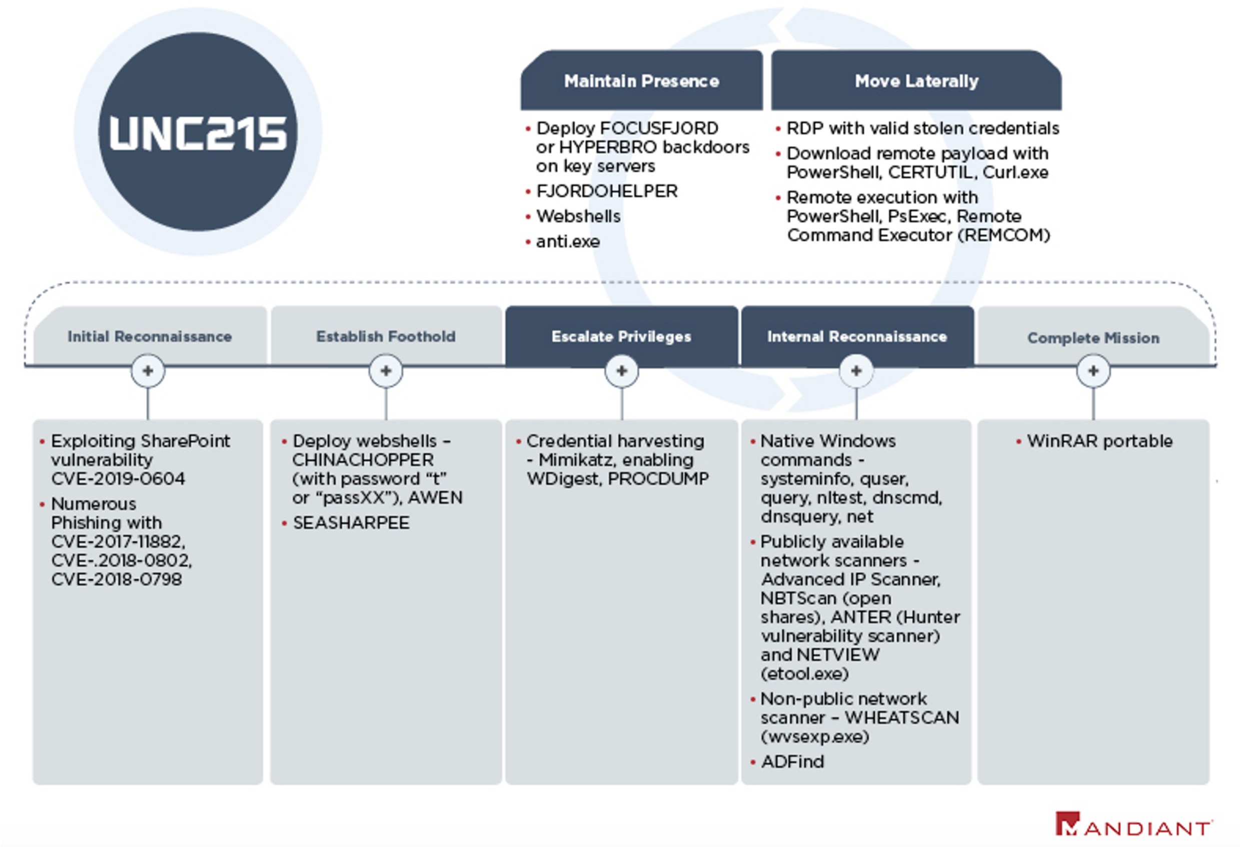

UNC215
Maintain Presence
• Deploy FOCUSFJORD or HYPERBRO backdoors on key servers
• FJORDOHELPER
• Webshells
• anti.exe
Move Laterally
• RDP with valid stolen credentials
• Download remote payload with PowerShell, CERTUTIL, Curl.exe
• Remote execution with PowerShell, PsExec, Remote Command Executor (REMCOM)
Initial Reconnaissance
• Exploiting SharePoint vulnerability CVE-2019-0604
• Numerous Phishing with CVE-2017-11882, CVE-.2018-0802, CVE-2018-0798
Establish Foothold
• Deploy webshells – CHINACHOPPER (with password "t" or "passXX"), AWEN
• SEASHARPEE
Escalate Privileges
• Credential harvesting - Mimikatz, enabling WDigest, PROCDUMP
Internal Reconnaissance
• Native Windows commands - systeminfo, quser, query, nltest, dnscmd, dnsquery, net
• Publicly available network scanners - Advanced IP Scanner, NBTScan (open shares), ANTER (Hunter vulnerability scanner) and NETVIEW (etool.exe)
• Non-public network scanner – WHEATSCAN (wvsexp.exe)
• ADFind
Complete Mission
• WinRAR portable
MANDIANT

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 (C2) 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 C2 and other configuration data. On initial execution, FOCUSFJORD writes its encrypted C2 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 C2 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.

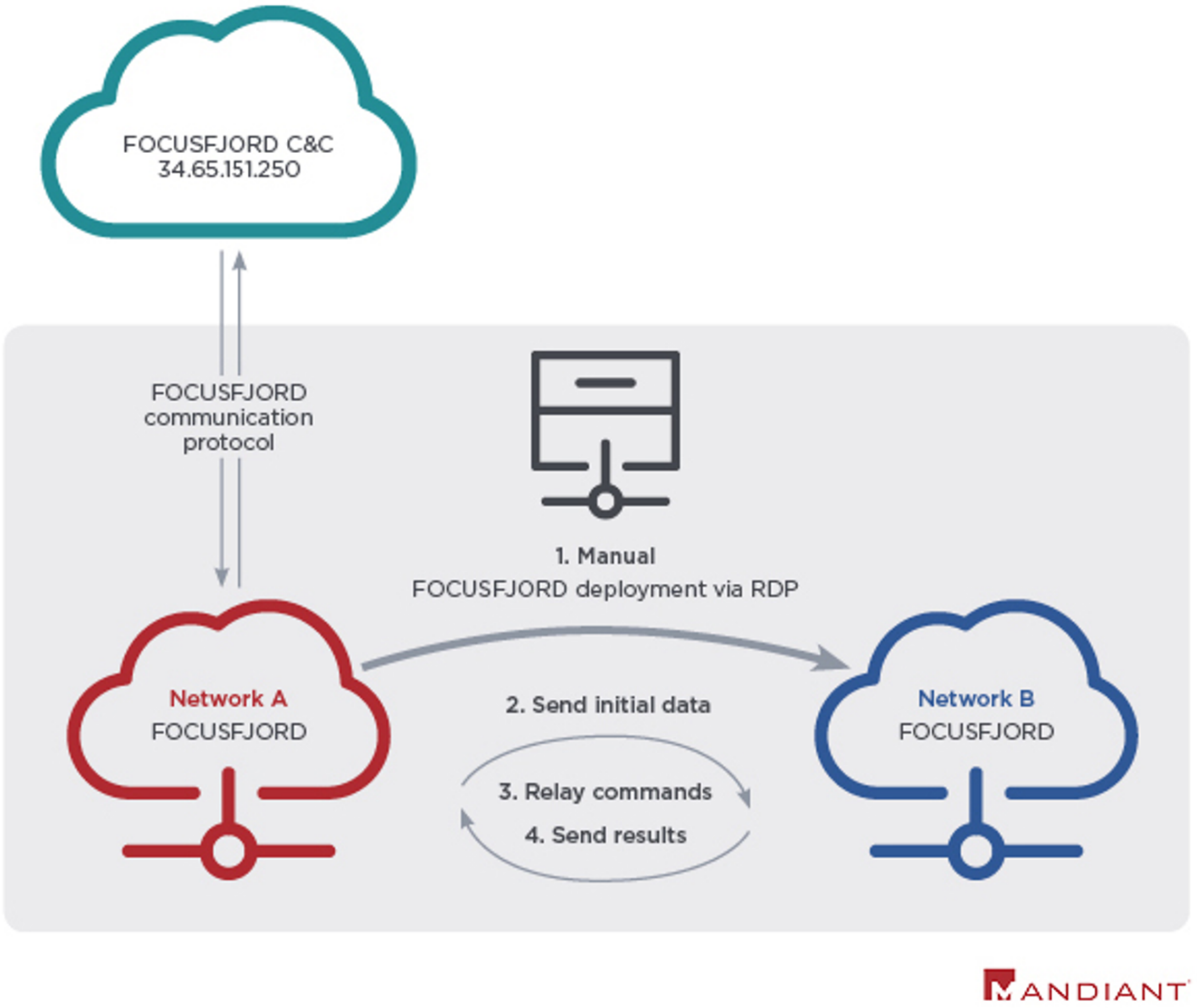


Figure 2: Two FOCUSFJORD samples configured to proxy C2 traffic

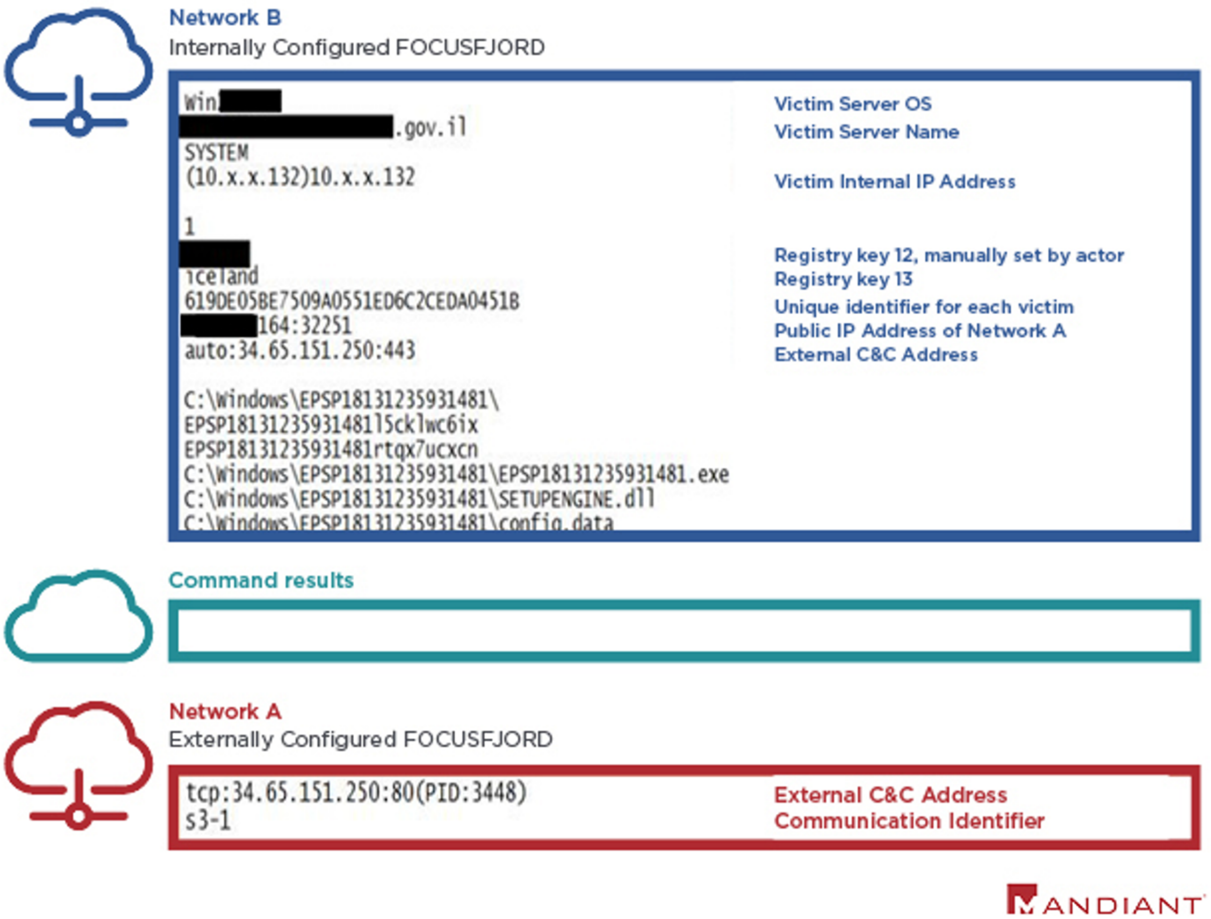
Concealing C2 Infrastructure

UNC215 made technical modifications to their tools to limit outbound network traffic and used other victim networks to proxy their C2 instructions, likely to minimize the risk of detection and blend in with normal network traffic. The following are examples of HYPERBRO and FOCUSFJORD samples capable of acting as proxies to relay communications to their C2 servers. We do not have enough context about the following samples to attribute all of them to UNC215, though they are representative of activity we have seen from the group.

- 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 C2 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 C2. 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 of a new malware (MD5: 625dd9048e3289f19670896cf5bca7d8) that shares code with FOCUSFJORD, but is distinct. However, analysis indicates that it only contains functions to relay communications between another FOCUSFJORD instance and a C2 server (Figure 2, Network A). We suspect this type of malware was used in the aforementioned operation. The actors stripped out unnecessary FOCUSFJORD capabilities, possibly to reduce the likelihood it would be detected by security controls. Figure 3 contains the data structure as it is being sent from a FOCUSFJORD sample configured to communicate with another FOCUSFJORD victim.



```
Win[redacted]
[redacted].gov.il
SYSTEM
(10.x.x.132)10.x.x.132

1
[redacted]
iceland
619DE05BE7509A0551ED6C2CEDA0451B
[redacted]164:32251
auto:34.65.151.250:443

C:\Windows\EPSP18131235931481\
EPSP18131235931481l5cklwc6ix
EPSP18131235931481rtqx7ucxcn
C:\Windows\EPSP18131235931481\EPSP18131235931481.exe
C:\Windows\EPSP18131235931481\SETUPENGINE.dll
C:\Windows\EPSP18131235931481\config.data
```

Victim Server OS
Victim Server Name
Victim Internal IP Address
Registry key 12, manually set by actor
Registry key 13
Unique identifier for each victim
Public IP Address of Network A
External C&C Address
Command results
Network A
Externally Configured FOCUSFJORD

```
tcp:34.65.151.250:80(PID:3448)
s3-1
```

Figure 3: Two FOCUSFJORD samples configured to proxy C2 traffic

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 C2 communications, there are two keys which 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 not clear 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 C2 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 (See 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.

[image needed]

Registry Key 13	FOCUSFJORD MD5 Hash	Related C2	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 (note: the * entries are from public reporting and have not been verified by Mandiant)

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.
- Around this time, the Turkish-language file Sosyal Güvenlik Reformu-Not-3.doc "Social Security Reform - Note - 3.doc" (MD5: 6930bd66a11e30dee1ef4f57287b1318) was distributed to a suspected Turkish government entity 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, C2 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 compartmentalization is not uncommon, but does show that UNC215 is relatively less concerned about the ability for their compromises to be linked to each other.
- C2 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 terminate EDR and Antivirus related services.

Attribution

Mandiant attributes this campaign to Chinese espionage operators which we track as UNC215 a Chinese espionage operation that has been suspected of targeting organizations around the world since at least 2014. We have low confidence that UNC215 is associated with APT27. UNC215 has compromised organizations in the government, technology, telecommunications, defense, finance, entertainment, and health care 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 in this post 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

Indicators of Compromise

The following indicators have been seen in use with the noted malware families, but not all have been confirmed to be used by UNC215.

Type	Value	Description
IP	85.204.74.143	HYPERBRO C2
IP	103.79.78.48	HYPERBRO C2
IP	89.35.178.105	HYPERBRO C2
IP	47.75.49.32	HYPERBRO C2
IP	139.59.81.253	FOCUSFJORD C2
IP	34.65.151.250	FOCUSFJORD C2
IP	159.89.168.83	FOCUSFJORD C2
IP	103.59.144.183	FOCUSFJORD C2
IP	141.164.52.232	FOCUSFJORD C2

Detecting the Techniques

FireEye detects this activity across our platforms.

Platform(s)	Detection Name

• Network Security • Email Security • Detection On Demand • Malware Analysis • File Protect	• Backdoor.Win32.HyperBro.FEC3 • FE_APT_Backdoor_Win32_HYPERBRO_1 • FE_Downloader_Win32_FOCUSFJORD_2 • FE_Trojan_Raw32_SILKWRAP_1 • Trojan.Win32.LuckyMouse.FEC3 • FE_Trojan_Raw32_SILKWRAP_1 • 33341691_APT.Downloader.Win.FOCUSFJORD • Trojan.Win32.DllHijack.FEC3 • FE_Trojan_Raw32_SILKWRAP_1 • FE_Autopatt_Win_FOCUSFJORD • Trojan.Generic • FE_Tool_Win_Generic_3 • FE_Tool_Win32_Generic_3 • FE_Trojan_Win_Generic_154 • FE_Trojan_Win32_Generic_403 • FE_Trojan_Win_Generic_155 • FE_Trojan_Win64_Generic_54 • FE_APT_Backdoor_Win32_HYPERBRO_2 • FE_Trojan_Win32_Generic_404 • FE_Trojan_Win32_Generic_406 • Suspicious File Config • Suspicious Regkey Added • Suspicious Process Launch Activity • Suspicious Codeinjection Activity • Suspicious Process Delete Activity • Suspicious Process Hijacking Activity • Suspicious Process Self Deletion Activity
Endpoint Security	• Generic.mg.a0b2193362152053 • Generic.mg.26d079e3afb08af0 • Generic.mg.28ce8dbdd2b7dfd1 • Generic.mg.04c51909fc65304d • Generic.mg.0e061265c0b59980 • Generic.mg.09ffc31a432f646e • Generic.mg.6ca8993b341bd90a • Generic.mg.0ec4d0a477ba21bd • Generic.mg.04dece2662f648f6 • Trojan.GenericKD.43427954 • Gen:Variant.Ursu.933105 • Trojan.GenericKD.32762213 • Trojan.GenericKD.34854595 • Gen:Variant.Ursu.256631 • Gen:Variant.Doina.16603 • Gen:Variant.Doina.13437

Helix	• 1.1.2927.fireeye_intel_hit_ip • 1.1.2928.fireeye_intel_hit_ip • 1.1.2929.fireeye_intel_hit_ip • 1.1.2930.fireeye_intel_hit_ip • 1.1.2947.fireeye_intel_hit_hash • 1.1.2948.fireeye_intel_hit_hash • 1.1.2949.fireeye_intel_hit_hash • 1.1.2950.fireeye_intel_hit_hash • 1.1.1404.windows_methodology_unusual_web_server_child_process • 1.1.3506.windows_methodology_adfind • 1.1.1650.windows_methodology_mimikatz_args • 1.1.1651.antivirus_methodology_mimikatz • 1.1.1652.windows_methodology_invokemimikatz_powershell_artifacts