Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

How ScarCruft APT group enhances its toolkit with a powerful Dolphin backdoor

Date of Publication	Admiralty Code	TA Number
December 1, 2022	A1	TA2022276

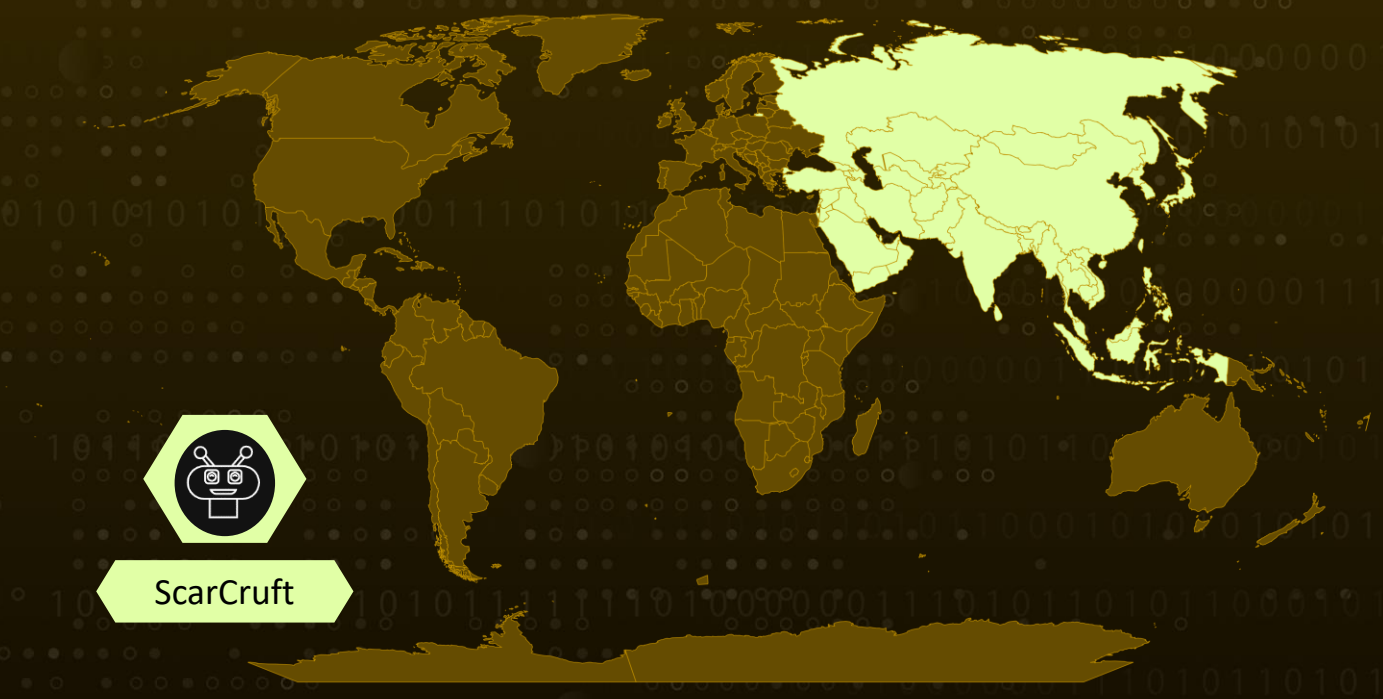
Summary

Active since: 2012
Attack Region: South Korea and Asian countries
Targeted Industry: Government and Military Organizations
Threat Actor: ScarCruft
Attack: Spying capabilities, which include monitoring drives and portable devices and exfiltrating files of interest, keylogging and taking screenshots, and stealing credentials from browsers.

CVEs

CVE	NAME	PATCH
CVE-2020-1380	Remote code execution vulnerability	✓

Attack Regions



Attack Details

#1

ScarCurft aka Reaper, APT 37, Ricochet Chollima is North Korean espionage group, active since 2012. ScarCruft has targeted South Korea Newspaper with a watering hole attack in the last year.

#2

In this attack, they used BLUELIGHT backdoor as the final payload, and the Dolphin backdoor was deployed on specific victims by BLUELIGHT. Upon execution of payload on selected ones, it looks for important files on the drives of hacked systems and exfiltrates them to Google Drive.

#3

Since Dolphin was first discovered in April 2021, it has undergone various updates. Earlier Dolphin versions had the capability to change victims' signed-in Google and Gmail accounts' security settings, which is a unique feature. In the newer versions Dolphin even abuses cloud storage services for C&C communication as part of its enhancement backdoor's capabilities to evade detection.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0007 Discovery
TA0040 Impact	TA0003 Persistence	TA0006 Credential Access	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1189 Drive-by Compromise	T1059.006 Command and Scripting Interpreter: Python
T1059.007 Command and Scripting Interpreter: JavaScript	T1203 Exploitation for Client Execution	T1106 Native API	T1053.005 Scheduled Task/Job: Scheduled Task
T1547.001 Boot or Logon Autostart Execution: Registry Run	T1055.002 Process Injection: Portable Executable Injection	T1027 Obfuscated Files or Information	T1555.003 Credentials from Password Stores: Credentials fr
T1539 Steal Web Session Cookie	T1010 Application Window Discovery	T1083 File and Directory Discovery	T1082 System Information Discovery
T1016 System Network Configuration Discovery	T1033 System Owner/User Discovery	T1124 System Time Discovery	T1056.001 Input Capture: Keylogging
T1560.002 Archive Collected Data: Archive via Library	T1119 Automated Collection	T1005 Data from Local System	T1025 Data from Removable Media
T1074.001 Data Staged: Local Data Staging	T1113 Screen Capture	T1071.001 Application Layer Protocol: Web Protocols	T1020 Automated Exfiltration

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	F9F6C0184CEE9C1E4E15C2A73E56D7B927EA685B 5B70453AB58824A65ED0B6175C903AA022A87D6A 21CA0287EC5EAEE8FB2F5D0542E378267D6CA0A6 D9A369E328EA4F1B8304B6E11B50275F798E9D6B 2C6CC71B7E7E4B28C2C176B504BC5BDB687C4D41

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1380

References

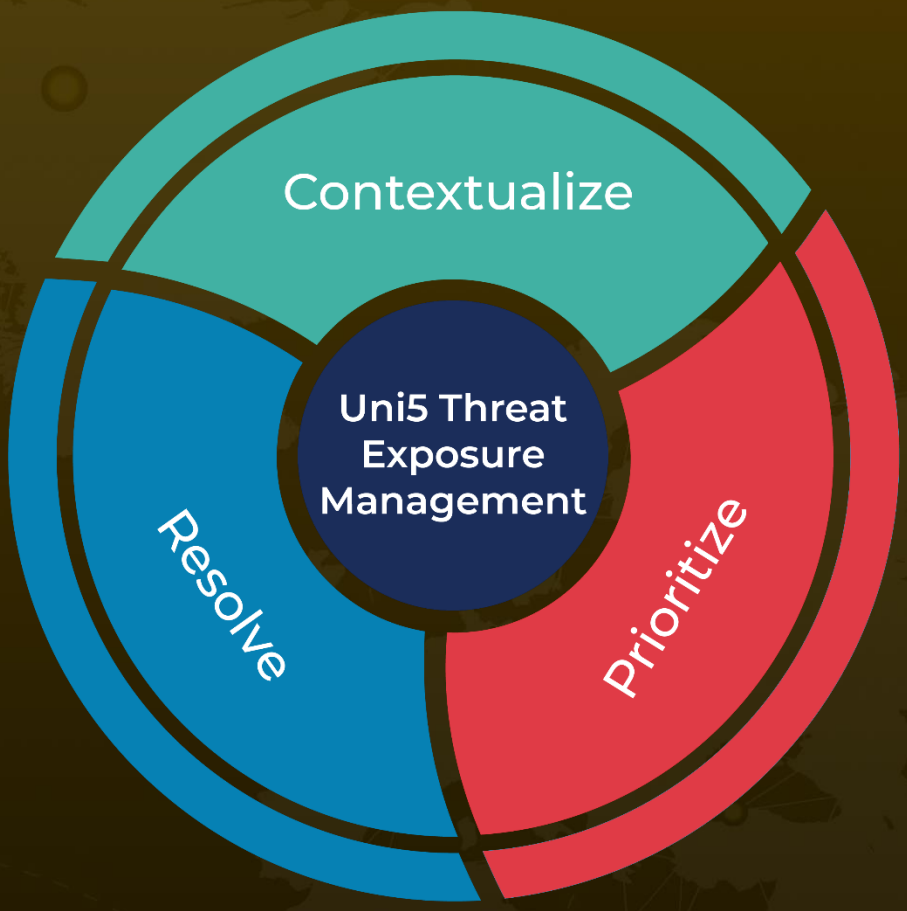
https://www.welivesecurity.com/2022/11/30/whos-swimming-south-korean-waters-meet-scarcrufts-dolphin/

https://www.hivepro.com/apt37-employs-konni-malware-to-target-high-level-organizations/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

December 1, 2022 . 7:42AM

More at www.hivepro.com