Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

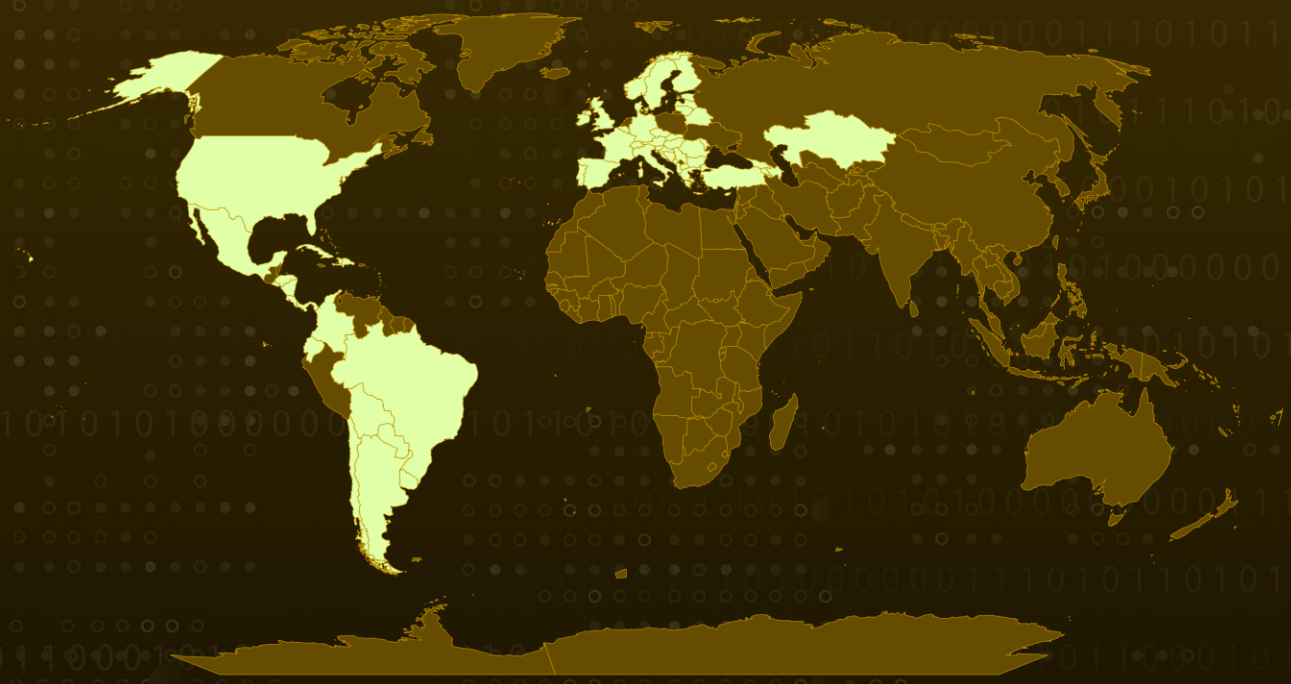
DoubleFinger A Sneaky Loader Targets Cryptocurrency

Date of Publication	Admiralty Code	TA Number
June 13, 2023	A1	TA2023261

Summary

First seen: 2023
Malware: DoubleFinger loader and GreetingGhoul stealer
Attack Region: Europe, the United States, and Latin America
Attack: A sophisticated campaign utilized an advanced multi-stage DoubleFinger loader to deploy the GreetingGhoul malware, which is designed to steal cryptocurrency credentials.

Attack Regions



Attack Details

#1 An advanced campaign utilizes a multi-stage DoubleFinger loader to deploy GreetingGhoul malware, specially crafted for pilfering cryptocurrency credentials. The campaign primarily targets entities in Europe, the United States, and Latin America. When the victim opens a malicious PIF attachment in an email message, they inadvertently trigger the deployment of DoubleFinger onto their machine, initiating the loader's initial stage.

#2 The legitimate Java binary is executed to load the second-stage shellcode. The third-stage shellcode employs low-level Windows API calls and maps ntdll.dll into the process memory, bypassing security solution hooks. Moving on to the fourth stage shellcode is relatively straightforward. It detects the presence of the fifth stage within itself and utilizes the Process Doppelgänging technique to execute it.

#3 The fifth stage creates a scheduled task that triggers the execution of the GreetingGhoul stealer. It's worth noting that DoubleFinger is not exclusive to cryptocurrency attacks; it has also been observed dropping Remcos RAT, a popular tool used by financially motivated cybercriminals.

Recommendations

Strengthen Security Measures: Given the advanced nature of the DoubleFinger loader and its ability to bypass security solution hooks, enhancing the existing security measures is crucial. This includes implementing robust endpoint protection systems that can detect and prevent the execution of malicious shellcodes.

Email Security: The campaign relies on social engineering tactics to trick victims into opening malicious email attachments. Organizations should conduct regular security awareness about the risks of opening unsolicited email attachments. Emphasize the importance of verifying the authenticity of email senders and practicing caution when interacting with email attachments, especially those in unfamiliar or suspicious formats like PIF files.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**T1560** Archive Collected Data	**T1053** Scheduled Task/Job	**T1574.002** DLL Side-Loading
T1129 Shared Modules	**T1055** Process Injection	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools
T1036 Masquerading	**T1497** Virtualization/Sandbox Evasion	**T1574** Hijack Execution Flow	**T1056** Input Capture
T1056.004 Credential API Hooking	**T1010** Application Window Discovery	**T1018** Remote System Discovery	**T1057** Process Discovery
T1082 System Information Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery	**T1104** Multi-Stage Channels
T1071 Application Layer Protocol	**T1095** Non-Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1571** Non-Standard Port
T1573 Encrypted Channel	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1055.013** Process Doppelgänging

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a500d9518bfe0b0d1c7f77343cac68d8 dbd0cf87c085150eb0e4a40539390a9a 56acd988653c0e7c4a5f1302e6c3b1c0 16203abd150a709c0629a366393994ea d9130cb36f23edf90848ffd73bd4e0e0 642f192372a4bd4fb3bfa5bae4f8644c a9a5f529bf530d0425e6f04cbe508f1e
Domain	cryptohedgefund[.]us

References

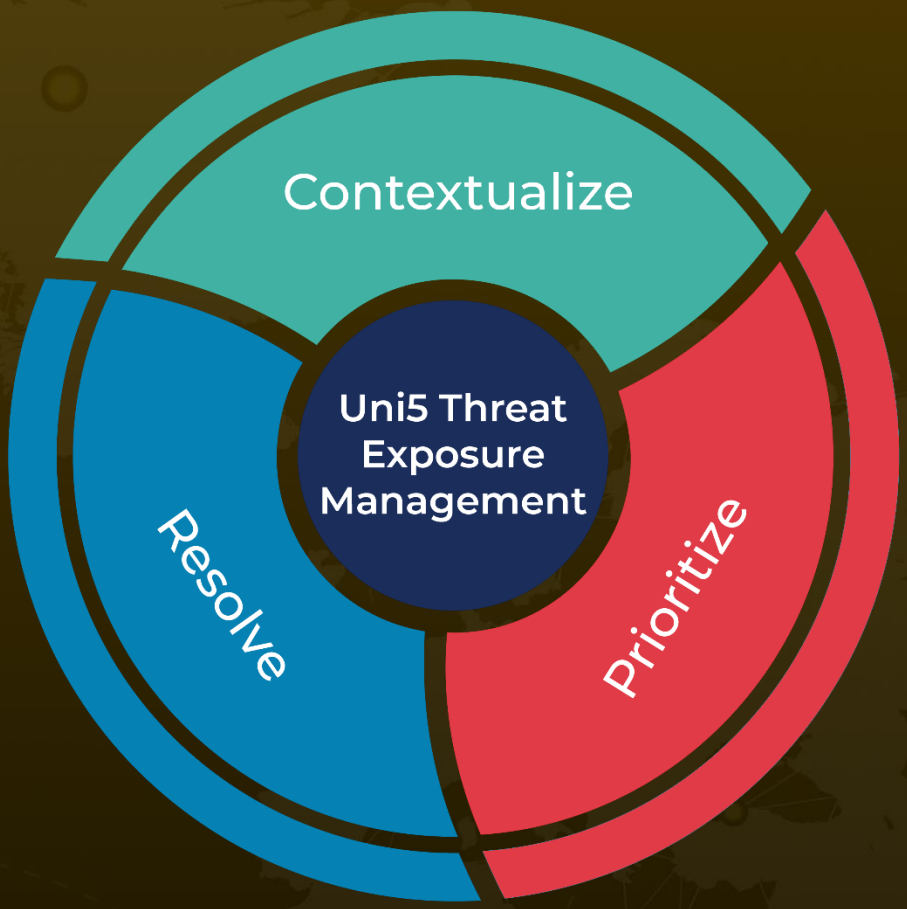
https://securelist.com/doublefinger-loader-delivering-greetingghoul-cryptocurrency-stealer/109982/

https://www.darkreading.com/attacks-breaches/new-loader-delivering-spyware-via-image-steals-cryptocurrency-info

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**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 13, 2023 • 5:48 AM

More at www.hivepro.com