Jul 12 2023

NETMANAGEIT

Intelligence Report

Diplomats Beware: Cloaked Ursa Phishing With a Twist

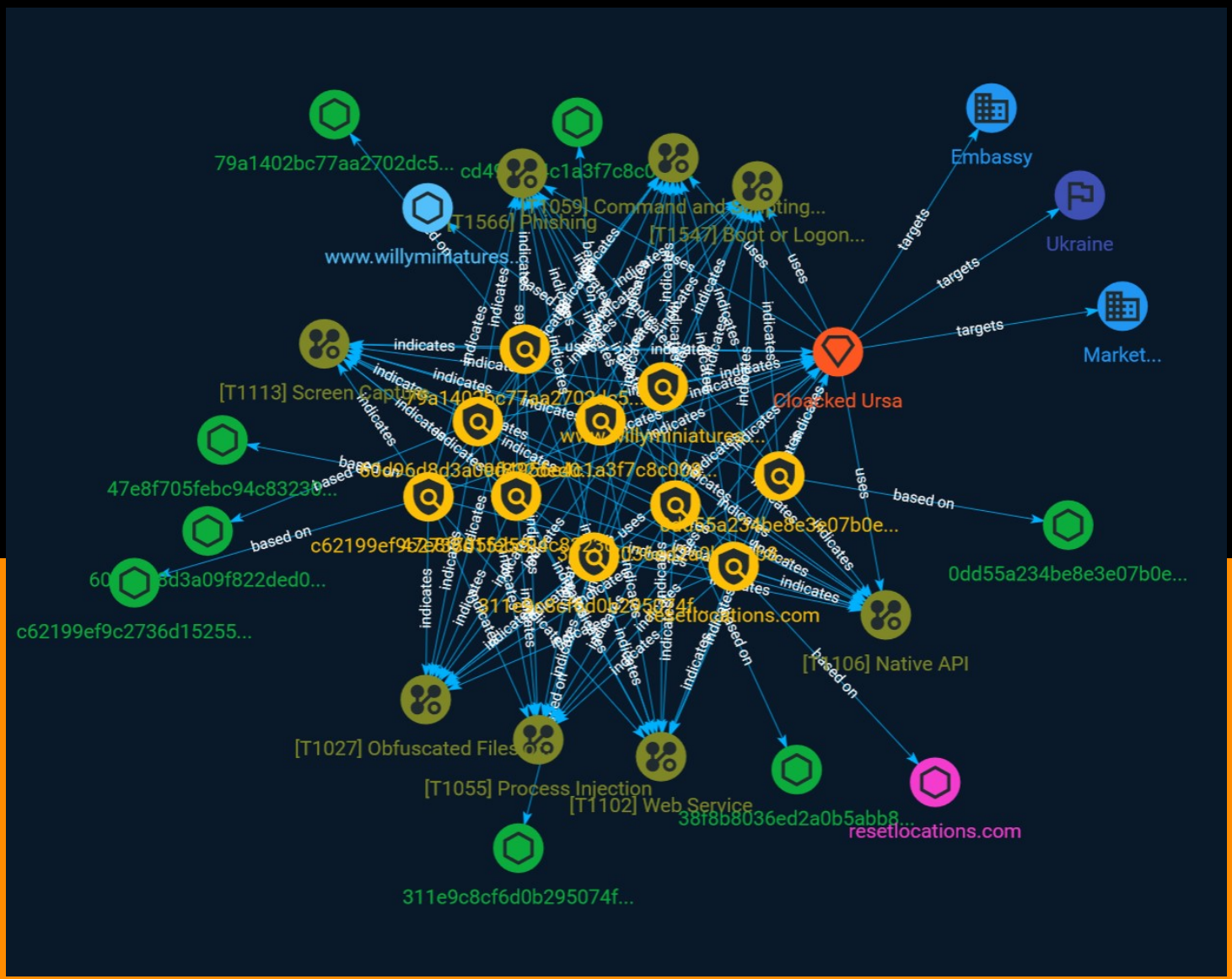

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Russian hackers known as Cloaked Ursa are targeting diplomatic missions around the world by leveraging the legitimate sale of a used BMW 5-series sedan in Ukraine, according to Palo Alto Networks Unit 42 researchers.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd917f60d9f1d8f18d07c26b1534
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd917f60d9f1d8f18d07c26b1534']
Name
cd4956e4c1a3f7c8c008c4658bb9eba7169aa874c55c12fc748b0ccfe0f4a59a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'cd4956e4c1a3f7c8c008c4658bb9eba7169aa874c55c12fc748b0ccfe0f4a59a']
Name

79a1402bc77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79a1402bc77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417f']

Name

resetlocations.com

Pattern Type

stix

Pattern

[domain-name:value = 'resetlocations.com']

Name

c62199ef9c2736d15255f5deaa663158a7bb3615ba9262eb67e3f4adada14111

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c62199ef9c2736d15255f5deaa663158a7bb3615ba9262eb67e3f4adada14111']

Name

www.willyminiatures.com

Pattern Type

stix

Pattern

[hostname:value = 'www.willyminiatures.com']

Name

311e9c8cf6d0b295074ffefaa9f277cb1f806343be262c59f88fbdf6fe242517

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '311e9c8cf6d0b295074ffefaa9f277cb1f806343be262c59f88fbdf6fe242517']

Name

60d96d8d3a09f822ded0a3c84194a5d88ed62a979cbb6378545b45b04353bb37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '60d96d8d3a09f822ded0a3c84194a5d88ed62a979cbb6378545b45b04353bb37']

Name

0dd55a234be8e3e07b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0dd55a234be8e3e07b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839']

Name

47e8f705febc94c832307dbf3e6d9c65164099230f4d438f7fe4851d701b580b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47e8f705febc94c832307dbf3e6d9c65164099230f4d438f7fe4851d701b580b']

Intrusion-Set

Name
Cloacked Ursa

Sector

Name
Market infrastructures
Description
Encompasses all the systems necessary for the smooth process of market financing operations. Are included payment systems, clearing houses, central securities depositories, securities settlement systems and trade repositories.
Name
Embassy

Country

Name
Ukraine

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
Name
Process Injection
ID
T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL,

download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for

adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Domain-Name

Value
resetlocations.com

StixFile

Value
47e8f705febc94c832307dbf3e6d9c65164099230f4d438f7fe4851d701b580b
311e9c8cf6d0b295074ffefaa9f277cb1f806343be262c59f88fbdf6fe242517
79a1402bc77aa2702dc5dca660ca0d1bf08a2923e0a1018da70e7d7c31d9417f
0dd55a234be8e3e07b0eb19f47abe594295889564ce6a9f6e8cc4d3997018839
60d96d8d3a09f822ded0a3c84194a5d88ed62a979cbb6378545b45b04353bb37
cd4956e4c1a3f7c8c008c4658bb9eba7169aa874c55c12fc748b0ccfe0f4a59a
38f8b8036ed2a0b5abb8fbf264ee6fd2b82dcd917f60d9f1d8f18d07c26b1534
c62199ef9c2736d15255f5deaa663158a7bb3615ba9262eb67e3f4adada14111

Hostname

Value
www.willyminiatures.com

External References

- https://otx.alienvault.com/pulse/64aed22c405b3e8f605125e8
- https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/