

Table of contents

Overview

● Description	4
● Confidence	4

Entities

● Indicator	5
● Intrusion-Set	15
● Malware	16
● Country	17
● Attack-Pattern	18

Observables

● Domain-Name	27
● Hostname	29



External References

-
- External References

30

Overview

Description

A toolkit that helps cybercriminals scam people on online marketplaces has been uncovered by ESET Research and is being used by a group of scammers in Russia, Ukraine and Uzbekistan.

Confidence

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

15 / 100

Indicator

Name

kufar.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'kufar.id7423.ru']

Name

id23352352.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id23352352.ru']

Name

id2918.site

Pattern Type

stix

Pattern

[domain-name:value = 'id2918.site']

Name

avito.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'avito.id7423.ru']

Name

2cdx.site

Pattern Type

stix

Pattern

[domain-name:value = '2cdx.site']

Name

olx.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'olx.id7423.ru']

Name

id2770.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id2770.ru']

Name

id7423.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id7423.ru']

Name

avito-rent.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'avito-rent.id7423.ru']

Name

pay-sacure4ds.ru

Pattern Type

stix

Pattern

[domain-name:value = 'pay-sacure4ds.ru']

Name

id83792.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id83792.ru']

Name

youla.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'youla.id7423.ru']

Name

id39103.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id39103.ru']

Name

id82567.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id82567.ru']

Name

id8092.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id8092.ru']

Name

id0391.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id0391.ru']

Name

kufar.by

Pattern Type

stix

Pattern

[domain-name:value = 'kufar.by']

Name

boxberry.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'boxberry.id7423.ru']

Name

formaa.ga

Pattern Type

stix

Pattern

[domain-name:value = 'formaa.ga']

Name

izi.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'izi.id7423.ru']

Name

smshub.org

Pattern Type

stix

Pattern

[domain-name:value = 'smshub.org']

Name

cdek.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'cdek.id7423.ru']

Name

youla.ru

Pattern Type

stix

Pattern

[domain-name:value = 'youla.ru']

Name

smscab.ru

Pattern Type

stix

Pattern

[domain-name:value = 'smscab.ru']

Name

3inf.site

Pattern Type

stix

Pattern

[domain-name:value = '3inf.site']

Name

id66410.ru

Pattern Type

stix

Pattern

[domain-name:value = 'id66410.ru']

Name

sbazar.id7423.ru

Pattern Type

stix

Pattern

[hostname:value = 'sbazar.id7423.ru']

Intrusion-Set

Name

Neanderthal

Malware

Name

Telegram

Name

Neanderthal

Name

Telekopye

Country

Name

Uzbekistan

Name

Russian Federation

Name

Ukraine

Attack-Pattern

Name

Compromise Accounts

ID

T1586

Description

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. [Establish Accounts](https://attack.mitre.org/techniques/T1585)), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. A variety of methods exist for compromising accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.(Citation: AnonHBGary) (Citation: Microsoft DEV-0537) Prior to compromising accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, etc.). Compromised accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos. Adversaries may directly leverage compromised email accounts for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).

Name

Establish Accounts

ID

T1585

Description

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity. (Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) For operations incorporating social engineering, the utilization of an online persona may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establishing a persona may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) Establishing accounts can also include the creation of accounts with email providers, which may be directly leveraged for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1)

Name

Gather Victim Identity Information

ID

T1589

Description

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal

data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](<https://attack.mitre.org/techniques/T1598>). Information about users could also be enumerated via other active means (i.e. [Active Scanning](<https://attack.mitre.org/techniques/T1595>)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](<https://attack.mitre.org/techniques/T1593/001>) or [Search Victim-Owned Websites](<https://attack.mitre.org/techniques/T1594>)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](<https://attack.mitre.org/techniques/T1593>) or [Phishing for Information](<https://attack.mitre.org/techniques/T1598>)), establishing operational resources (ex: [Compromise Accounts](<https://attack.mitre.org/techniques/T1586>)), and/or initial access (ex: [Phishing](<https://attack.mitre.org/techniques/T1566>) or [Valid Accounts](<https://attack.mitre.org/techniques/T1078>)).

Name

Develop Capabilities

ID

T1587

Description

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: Bitdefender StrongPity June 2020)(Citation: Talos Promethium June 2020) As with legitimate development efforts, different skill sets may be required for developing capabilities. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's development capabilities,

provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the capability.

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](<https://attack.mitre.org/techniques/T1090>).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture

mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

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

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install

configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction. (Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions. (Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control. (Citation: Chrome Extension C2 Malware)

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

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

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

smshub.org

id2770.ru

id39103.ru

youla.ru

id23352352.ru

smscab.ru

id2918.site

formaa.ga

pay-sacure4ds.ru

id8092.ru

2cdx.site

id7423.ru

3inf.site

id82567.ru

id83792.ru

id0391.ru

id66410.ru

kufar.by

Hostname

Value

cdek.id7423.ru

izi.id7423.ru

kufar.id7423.ru

avito.id7423.ru

sbazar.id7423.ru

olx.id7423.ru

boxberry.id7423.ru

youla.id7423.ru

avito-rent.id7423.ru

External References

-
- <https://otx.alienvault.com/pulse/64e86689b62dbbf6491d9a92>
-
- <https://www.welivesecurity.com/en/eset-research/telekopye-hunting-mammoths-using-telegram-bot/>