Oct 15 2023

NETMANAGEIT

Intelligence Report

DarkGate Opens Organizations for Attack via Skype, Teams

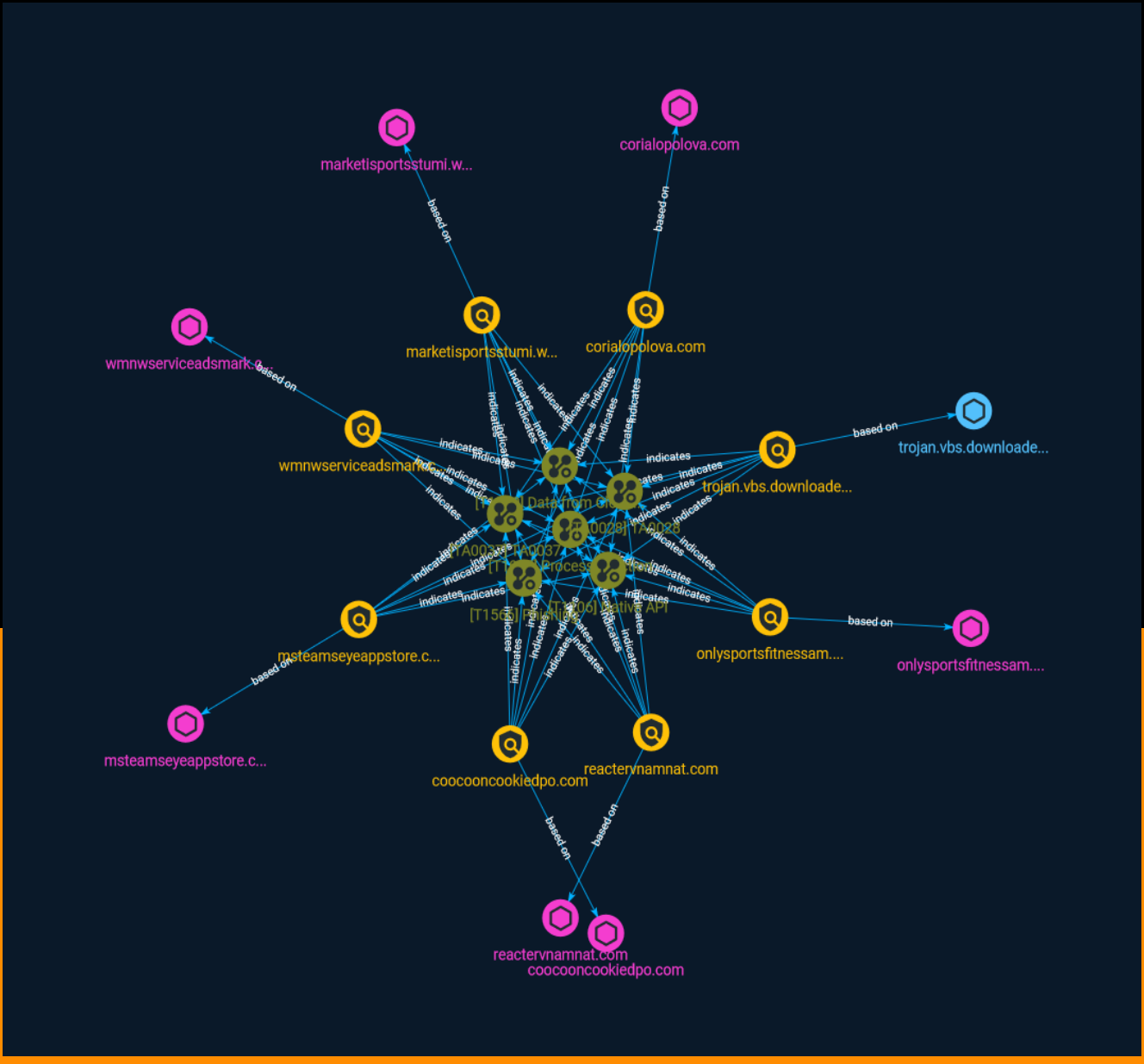

Table of contents

Overview

Entities

Observables

External References

Overview

Description

From July to September, we observed the DarkGate campaign (detected by Trend Micro as TrojanSpy.AutoIt.DARKGATE.AA) abusing instant messaging platforms to deliver a VBA loader script to victims. This script downloaded and executed a second-stage payload consisting of a AutoIT scripting containing the DarkGate malware code. It's unclear how the originating accounts of the instant messaging applications were compromised, however is hypothesized to be either through leaked credentials available through underground forums or the previous compromise of the parent organization.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

Data from Cloud Storage

ID

T1530

Description

Adversaries may access data from improperly secured cloud storage. Many cloud service providers offer solutions for online data object storage such as Amazon S3, Azure Storage, and Google Cloud Storage. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider's APIs. In other cases, SaaS application providers such as Slack, Confluence, and Salesforce also provide cloud storage solutions as a peripheral use case of their platform. These cloud objects can be extracted directly

from their associated application.(Citation: EA Hacked via Slack - June 2021)(Citation: SecureWorld - How Secure Is Your Slack Channel - Dec 2021)(Citation: HackerNews - 3 SaaS App Cyber Attacks - April 2022)(Citation: Dark Clouds_Usenix_Mulazzani_08_2011) Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.(Citation: Amazon S3 Security, 2019)(Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019) There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions. This open access may expose various types of sensitive data, such as credit cards, personally identifiable information, or medical records.(Citation: Trend Micro S3 Exposed PII, 2017) (Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017) (Citation: Rclone-mega-extortion_05_2021) Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

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
TA0037
ID
TA0037
Name
TA0028
ID
TA0028

Indicator

Name
coocooncookiedpo.com
Pattern Type
stix
Pattern
[domain-name:value = 'coocooncookiedpo.com']
Name
marketisportsstumi.win
Pattern Type
stix
Pattern
[domain-name:value = 'marketisportsstumi.win']
Name
onlysportsfitnessam.com

Pattern Type
stix
Pattern
[domain-name:value = 'onlysportsfitnessam.com']
Name
msteamseyeappstore.com
Pattern Type
stix
Pattern
[domain-name:value = 'msteamseyeappstore.com']
Name
corialopolova.com
Pattern Type
stix
Pattern
[domain-name:value = 'corialopolova.com']
Name
reactervnamnat.com

Pattern Type
stix
Pattern
[domain-name:value = 'reactervnamnat.com']
Name
wmnwserviceadsmark.com
Pattern Type
stix
Pattern
[domain-name:value = 'wmnwserviceadsmark.com']
Name
trojan.vbs.downloader.ae
Pattern Type
stix
Pattern
[hostname:value = 'trojan.vbs.downloader.ae']

Domain-Name

Value
reactervnamnat.com
onlysportsfitnessam.com
coocooncookiedpo.com
corialopolova.com
wmnwserviceadsmark.com
msteamseyeappstore.com
marketisportsstumi.win

Hostname

Value
trojan.vbs.downloader.ae

External References

- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams/IOCs-DarkGate-Opens-Organizations-for-Attack-via-Skype-Teams.txt
- https://otx.alienvault.com/pulse/6529aae9ade1038d1ea076c6
- https://www.trendmicro.com/en_us/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams.html