Oct 28 2023

NETMANAGEIT

Intelligence Report

Sticky Werewolf spies attack government organizations in Russia and Belarus

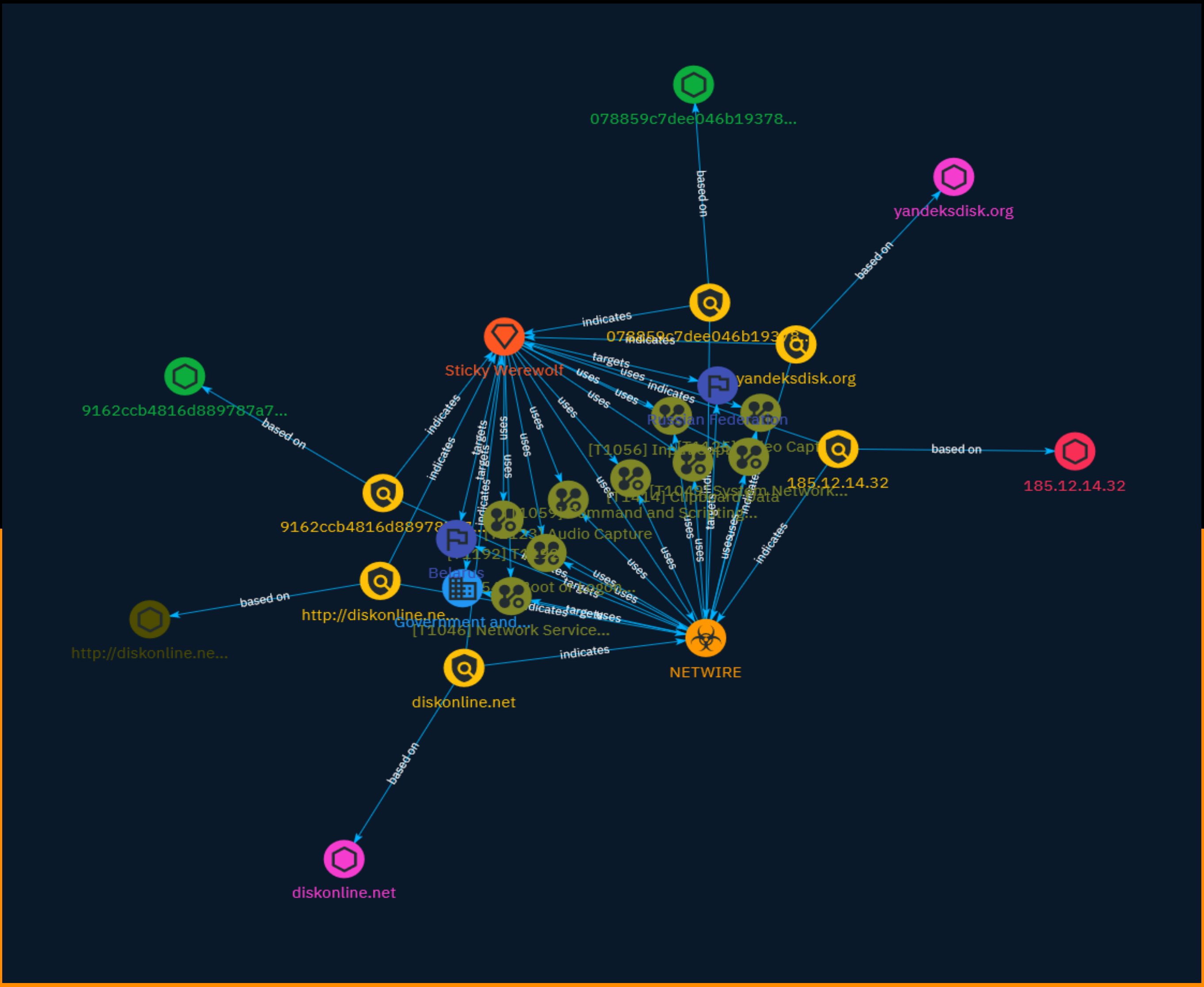

Table of contents

Overview

Entities

Observables

External References

Overview

Description

BI.ZONE cyber intelligence specialists have discovered a new group that uses legitimate software to interfere with the work of government organizations. A characteristic feature of this criminal community, called Sticky Werewolf, is the use of fairly popular, commercially available tools that are easy to detect and block. This has not stopped Sticky Werewolf from achieving success: the group has been active since at least April 2023 and has carried out at least 30 attacks to date.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Clipboard Data

ID

T1414

Description

Adversaries may abuse clipboard manager APIs to obtain sensitive information copied to the device clipboard. For example, passwords being copied and pasted from a password manager application could be captured by a malicious application installed on the device.(Citation: Fahl-Clipboard) On Android, applications can use the `ClipboardManager.OnPrimaryClipChangedListener()` API to register as a listener and monitor the clipboard for changes. However, starting in Android 10, this can only be used if the application is in the foreground, or is set as the device’s default input method editor (IME).(Citation: Github Capture Clipboard 2019)(Citation: Android 10 Privacy Changes) On iOS, this can be accomplished by accessing the `UIPasteboard.general.string` field. However, starting in iOS 14, upon accessing the clipboard, the user will be shown a system notification if the accessed text originated in a different application. For example, if the user copies the text of an iMessage from the Messages application, the notification will read “application_name has pasted from Messages” when the text was pasted in a different application.(Citation: UIPPasteboard)

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

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

Audio Capture

ID

T1123

Description

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Name

T1192

ID

T1192

Name

Video Capture

ID

T1125

Description

An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture video or images. Video or image files may be written to disk and exfiltrated later. This technique differs from [Screen Capture](https://attack.mitre.org/techniques/T1113) due to use of specific devices or applications for video recording rather than capturing the victim's screen. In macOS, there are a few different malware samples that record the user's webcam such as FruitFly and Proton. (Citation: objective-see 2017 review)

Name

Network Service Discovery

ID

T1046

Description

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021) Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well. Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host’s registered services on the network. For example, adversaries can use a mDNS query (such as `dns-sd -B _ssh._tcp .`) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

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

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name

diskonline.net

Pattern Type

stix

Pattern

[domain-name:value = 'diskonline.net']

Name

9162ccb4816d889787a7e25ba680684afca1d7f3679c856ceedaf6bf8991e486

Description

Netwire

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9162ccb4816d889787a7e25ba680684afca1d7f3679c856ceedaf6bf8991e486']

Name

yandeksdisk.org

Pattern Type

stix

Pattern

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

Name

http://diskonline.net/poryadok-deystviy-i-opoveshcheniya-grazhdanskoy-oborony.pdf

Pattern Type

stix

Pattern

[url:value = 'http://diskonline.net/poryadok-deystviy-i-opoveshcheniya-grazhdanskoy-oborony.pdf']

Name

078859c7dee046b193786027d5267be7724758810bdbc2ac5dd6da0ebb4e26bb

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '078859c7dee046b193786027d5267be7724758810bdbc2ac5dd6da0ebb4e26bb']
Name
185.12.14.32
Description
Netwire CC=NL ASN=AS50673 Serverius Holding B.V.
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.12.14.32']

Intrusion-Set

Name
Sticky Werewolf

Country

Name
Belarus

Name
Russian Federation

Malware

Name
NETWIRE

Description
[NETWIRE](https://attack.mitre.org/software/S0198) is a publicly available, multiplatform remote administration tool (RAT) that has been used by criminal and APT groups since at least 2012.(Citation: FireEye APT33 Sept 2017)(Citation: McAfee Netwire Mar 2015)(Citation: FireEye APT33 Webinar Sept 2017)

Domain-Name

Value
diskonline.net
yandeksdisk.org

StixFile

Value
078859c7dee046b193786027d5267be7724758810bdbc2ac5dd6da0ebb4e26bb
9162ccb4816d889787a7e25ba680684afca1d7f3679c856ceedaf6bf8991e486

IPv4-Addr

Value
185.12.14.32

Url

Value
http://diskonline.net/poryadok-deystviy-i-opoveshcheniya-grazhdanskoy-oborony.pdf

External References

- https://otx.alienvault.com/pulse/652d5b9da7b9aa36c8faefb4
- https://bi.zone/expertise/blog/shpiony-sticky-werewolf-atakuyut-gosudarstvennye-organizatsii-rossii-i-belarusi/