

# NETMANAGEIT

## Intelligence Report

# GHOSTPULSE haunts victims using defense evasion bag o' tricks



# Table of contents

---

## Overview

---

● Description	4
● Confidence	4
● Content	5

---

## Entities

---

● Attack-Pattern	6
------------------	---

---

## Observables

---

● Domain-Name	14
● StixFile	15
● IPv4-Addr	16



## External References

- 
- External References

17

# Overview

## Description

Elastic Security Labs has observed a campaign to compromise users with signed MSIX application packages to gain initial access. The campaign leverages a stealthy loader we call GHOSTPULSE which decrypts and injects its final payload to evade detection.

## Confidence

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

15 / 100

# Content

N/A

# Attack-Pattern

**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 abusible system utilities to evade security monitoring is also a form of [Masquerading](<https://attack.mitre.org/techniques/T1036>). (Citation: LOLBAS Main Site)

**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**

Subvert Trust Controls

**ID**

T1553

**Description**

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [Modify Registry](<https://attack.mitre.org/techniques/T1112>) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

**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**

Archive Collected Data

**ID**

T1560

**Description**

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

**Name**

Event Triggered Execution

**ID**

T1546

**Description**

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events. (Citation: Backdooring an AWS account)(Citation: Varonis Power Automate Data Exfiltration) (Citation: Microsoft DART Case Report 001) Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked. (Citation: FireEye WMI 2015)(Citation: Malware Persistence on OS X)(Citation: amnesia malware) Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

**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**

Deobfuscate/Decode Files or Information

**ID**

T1140

**Description**

Adversaries may use [Obfuscated Files or Information](<https://attack.mitre.org/techniques/T1027>) to hide artifacts of an intrusion from analysis. They may require

separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

**Name**

Stage Capabilities

**ID**

T1608

**Description**

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): \* Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) \* Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) \*

Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](<https://attack.mitre.org/techniques/T1105>). (Citation: Volexity Ocean Lotus November 2020) \* Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](<https://attack.mitre.org/techniques/T1573/002>) with [Web Protocols](<https://attack.mitre.org/techniques/T1071/001>)). (Citation: DigiCert Install SSL Cert)

# Domain-Name

## Value

manoj Singh Negi.com

# StixFile

## Value

4283563324c083f243cf9335662ecc9f1ae102d619302c79095240f969d9d356

eb2addefd7538cbd6c8eb42b70cafe82ff2a8210e885537cd94d410937681c61

0c01324555494c35c6bbd8babd09527bfc49a2599946f3540bb3380d7bec7a20

49e6a11453786ef9e396a9b84aeb8632f395477abc38f1862e44427982e8c7a9

ee4c788dd4a173241b60d4830db128206dcfb68e79c68796627c6d6355c1d1b8

# IPv4-Addr

## Value

195.201.198.179

78.24.180.93



# External References

- 
- <https://otx.alienvault.com/pulse/653fe482a1235f71266181a8>
- 
- <https://www.elastic.co/security-labs/ghostpulse-haunts-victims-using-defense-evasion-bag-o-tricks>