Security Incident Report

SHERLOCK: *Unit42*

Ielon Raykhelson

www.ielonraykhelson.org

May 6, 2026

Version: 1.1 - Updated MITRE ATT&CK mappings

Table of Contents

1 Disclaimer and Attribution Notice

The contents and structure of this document are based on a template originally developed by Hack The Box (HTB). All modifications herein have been made by the author solely for personal, educational, and non-commercial purposes. The author does not claim ownership of the original template or any HTB intellectual property.

This document is intended solely for reporting findings from Hack The Box training challenges and does not pertain to any real-world company, system, or infrastructure. No portion of this document may be represented as official HTB material, and all references to HTB are for attribution purposes only.

2 Engagement Contacts

Contacts		
Primary Contact	**Title**	**Contact Email**
Ielon Raykhelson	Lead Security Analyst	raykhelson.ielon@gmail.com

3 Executive Summary

Ielon Raykhelson was engaged to investigate a security incident on host `DESKTOP-887GK2L` involving user `CyberJunkie`. The objective is to identify the root cause and the full extent of this incident and to meticulously document the findings in an understandable, technically robust, and reproducible way.

UltraVNC Malware Compromise

Incident ID: INC001-001

Incident Severity: Medium

Incident Status: **Complete**

Incident Overview:

On February 14th, 2024, user `CyberJunkie` on host `DESKTOP-887GK2L` downloaded a malicious executable, `Preventivo24.02.14.exe.exe`, via Mozilla Firefox from a Dropbox-hosted link. After execution, the malware dropped multiple payload files to the disk. The malware performed timestomping to alter the creation time of a file, issued a connectivity check, established a VNC-based remote access connection to an externally-controlled server, and performed forensic evidence destruction.

Key Findings:

A trojanized UltraVNC installer was downloaded via Mozilla Firefox from a malicious Dropbox link, potentially originating from a malicious email. Upon execution, a decoy PDF, several command scripts, and a copy of the UltraVNC's executable were downloaded to a hidden directory within `AppData`. The malware performed timestomping on the decoy PDF to alter its creation time, issued an HTTP connectivity check to `www.example.com:80`, and established a VNC communication channel to `vnvariant2024.ddnsfree[.]com:5500`. Although no data exfiltration was confirmed, the establishment of a malicious VNC session presents a significant risk to data and operational confidentiality.

Immediate Actions:

All related hashes of `Preventivo24.02.14.exe.exe` and its dropped files should be added as known IOC's to endpoint detection and alerting platforms. As no CVE was exploited, resulting in the compromise, there are no directly related vulnerabilities to patch. It is recommended to implement User Behavioral Analytics (UBA) and Endpoint Detection and Response (EDR) platforms; however, if these systems were already in place, they should be reevaluated, tuned, and verified to detect and address double-extension executables, timestomping, and anomalous VNC traffic. Additionally, browser-level controls or a web proxy may be considered to restrict downloads from file-sharing platforms, such as Dropbox, where it is not operationally required.

Stakeholder Impact:

No organization was identified as an affected entity in this incident -- the compromise was evident to affect only `CyberJunkie:DESKTOP-887GK2L`. The established VNC session enabled the attacker to view the compromised system's screen in real time, potentially jeopardizing data and operational confidentiality as they are related to the compromised user and system. No evidence of data exfiltration was present.

4 Technical Analysis

UltraVNC Malware Compromise

Affected Systems & Data

Only a single system was identified as compromised during this incident:

`CyberJunkie:DESKTOP-887GK2L` -- No sensitive data stores were identified on the system; however, the establishment of an active VNC session suggests the compromise of data and operational confidentiality as they relate to user `CyberJunkie` and their system `DESKTOP-887GK2L`.

Evidence Sources & Analysis

*The primary evidence source for this investigation was the Windows Sysmon operational event log collected from `DESKTOP-887GK2L`, imported and analyzed within a local instance of the **Windows Event Viewer**. Other sources include **Unit42's** Threat Intelligence Report for the UltraVNC Infection, **VirusTotal's** Analysis of the Malicious Executable, and **Any.Run's** Sandbox Detonation of the Malicious Executable.*

The event log file was filtered using XML queries tailored toward specific Sysmon Event IDs relevant to each stage of the infection chain.

Download of the malicious File

To identify the origin of the malicious file, the Sysmon log was filtered for `EventID 15, FileCreateStreamHash`, which captures file stream creation and zone identifier metadata written during download.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[System[(EventID=15)]]
    </Select>
  </Query>
</QueryList>
```

Captured events indicated that, at `2024-02-14 03:31:26`, Mozilla Firefox downloaded `Preventivo24.02.14.exe.exe` from a Dropbox-hosted URL. The Zone.Identifier stream recorded the following:

- **ReferrerUrl**: `https://www.dropbox[.]com/`
- **HostUrl**: `https://uc2f030016253ec53f4953980a4e.dl.dropboxusercontent[.]com/cd/0/get/CNNlOCYTD8cqLXFQzXaeYHRkHg_PoR35Et2T0_IkqE5ijvkTAQNljV7ZkK2fLXWI2bJy944RnwKttvmNWpVd5olpBcffnvnL_IfEjzr65jZZUOxtWA9rSgJ1jc91IZILHVAJHgRhjpZYLtGo83_QbeInB7x2oEAoYg-JLF54zbhziQ/file`

This event confirms the malicious installer was delivered via Dropbox, which is consistent with the infection chain detailed within Unit42's threat intelligence documentation for this campaign.

File Creation at Download

To confirm the file was written to the disk by Mozilla Firefox, the Sysmon log was filtered for `EventID 11, FileCreate`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[System[(EventID=11)]]
    </Select>
  </Query>
</QueryList>
```

The returned events confirm that, at `2024-02-14 03:41:26`, Mozilla Firefox created the file at the path `C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe`.

Additionally, the double `.exe` extension is consistent with MITRE T1036.007 - Masquerading: Double File Extension as a defense evasion technique. There were 56 FileCreate events in total during the investigation window.

Mark-of-the-Web Removal

Following the attack pattern, the Sysmon log was filtered for `EventID 26, FileDeleteDetected`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[System[(EventID=26)]]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:56`, `Explorer.EXE` deleted the `Zone.Identifier` Alternate Data Stream (ADS) from `Preventivo24.02.14.exe.exe` immediately before its execution. As its removal occured before its execution, it is likely that the user manually allowed this file to be downloaded, unless there was another compromise which allowed it.

Its removal is consistent with MITRE T1553.005 - Subvert Trust Controls: Mark-of-the-Web Bypass.

Malware Execution

To identify the execution of the malicious installer, the Sysmon log was filtered for `EventID 1, ProcessCreate`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[System[(EventID=1)]]
    </Select>
  </Query>
</QueryList>
```

The returned events indicate that, at `2024-02-14 03:41:56`, `Preventivo24.02.14.exe.exe` was executed under ProcessID (PID) `10672`.

The following hashes were recorded:

- **MD5**: `32F35B78A3DC5949CE3C99F2981DEF6B`
- **SHA1**: `18A24AA0AC052D31FC5B56F5C0187041174FFC61`
- **SHA256**: `0CB44C4F8273750FA40497FCA81E850F73927E70B13C8F80CDCFEE9D1478E6F3`
- **IMPHASH**: `36ACA8EDDDB161C588FCF5AFDC1AD9FA`

The aforementioned hashes match those of the trojanized UltraVNC installer as documented in Unit 42's threat intelligence report for this campaign.

Additionally, the `EventID 7, ImageLoad` event list for this process revealed the following:

- The file's embedded metadata identified `Preventivo24.02.14.exe.exe` as `Fattura 2 2024.exe` ("Invoice 2 2024" in Italian) under the product name "Photo and vn" by the company "Photo and Fax Vn".
- The executable was unsigned, indicating its illegitimacy.

DLL Image Loads

To identify any suspicious DLL loading by the malware, the Sysmon log was filtered for `EventID 7, ImageLoad`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[
        System[(EventID=7)]
        and
        EventData[Data[@Name='ProcessId']='10672']
      ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:56`, Sysmon flagged PID `10672` loading itself as a DLL, tagged as MITRE T1574.002 - Hijack Execution Flow: DLL Sideloading. At `2024-02-14 03:41:56`, `urlmon.dll` was loaded, a legitimate Windows DLL used for URL handling and file downloads, which remains consistent with the observed network activity.

At `2024-02-14 03:41:57`, two `.NET runtime` DLLs were loaded by PID `10672`:

- `C:\Windows\SysWOW64\mscoree.dll`
- `C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll`

Sysmon tagged both events as MITRE T1055.001 - Process Injection: Dynamic-link Library Injection. While the loading of `.NET runtime` DLLs is not conclusive of process injection itself, it is, however, indicative of a malicious `.NET runtime` initialization. This potentially may have been to execute `.NET` managed code in memory. Additionally, no `EventID 8, CreateRemoteThread` events were identified that could directly confirm injection.

At `2024-02-14 03:41:58`, `taskschd.dll` was loaded by PID `10672` and tagged by Sysmon as MITRE T1053.005 - Scheduled Task/Job: Scheduled Task. This is indicative of a malicious interaction with the Windows Task Scheduler, strongly suggesting a persistence attempt via a scheduled task; however,

there were no explicitly corresponding `EventID 4, ServiceCreate` events identified to confirm task creation.

DNS Query

To identify DNS activity generated by the malware, the Sysmon log was filtered for `EventID 22, DNSEvent`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[System[(EventID=22)]]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:56`, ProcessID `10672` generated a DNS query for `www.example.com`. From Unit42's analysis, this query and address serve as a simple connectivity check and are not inherently malicious.

Network Connection

Following the discovery of a DNS query, the Sysmon log was filtered for `EventID 3, NetworkConnect` to identify outbound network connections established by the malware.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[System[(EventID=3)]]
        and
        EventData[Data[@Name='Image']='C:
\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe']
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:57`, ProcessID `10672` established an outbound network connection:

- **Source**: `172.17.79[.]132:61177`
- **Destination**: `93.184[.]216.34:80`

The Destination IP `93.184.216[.]34` resolves to `www.example[.]com`, confirming the connectivity check observed in the identified DNS query event.

Unit42's threat intelligence analysis of this malware documents the true VNC C2 channel as `vnvariant2024.ddnsfree[.]com:5500`; however, it was not captured in the Sysmon log, highlighting a visibility gap in the collected evidence.

Registry Activity

To identify registry modifications made by the malware, the Sysmon log was filtered for `EventID 12, RegistryEvent (CreateKey)` and `EventID 13, RegistryEvent (SetValue)`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
```

```
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[
        System[(EventID=12 or EventID=13)]
        and
        EventData[Data[@Name='ProcessId']='10672']
      ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:57`, ProcessID `10672` created two registry keys under `CyberJunkie`'s certificate stores:

- `HKU\S-1-5-21-3393683511-3463148672-371912004-1001\Software\Microsoft\SystemCertificates\Root\Certificates`
- `HKU\S-1-5-21-3393683511-3463148672-371912004-1001\Software\Microsoft\SystemCertificates\CA\Certificates`

These events follow patterns described in MITRE T1553.004 - Subvert Trust Controls: Install Root Certificate. The creation of registry keys in both the trusted root and CA certificate stores indicates malicious attempts to install certificates, possibly to suppress browser trust warnings or to enable the interception of TLS traffic during the VNC session.

Additionally, at `2024-02-14 03:41:57` and `2024-02-14 03:41:58`, two registry values were set under the Background Activity Moderator (BAM) key:

- `HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\[SID]\Device\HarddiskVolume3\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe`
- `HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\[SID]\Device\HarddiskVolume3\Windows\SysWOW64\msiexec.exe`

These BAM additions do not appear to explicitly serve as persistence mechanisms; however, they do forensically indicate the execution of both `Preventivo24.02.14.exe.exe` and `msiexec.exe` during the investigation window. It is also worth noting that, while Unit42 documents `on.cmd` as the primary persistence mechanism via a registry run key, no corresponding registry write events were captured within the Sysmon log for the `Preventivo24.02.14`, `on.cmd`, or any of their related artifacts.

Named Pipe Creation

To identify inter-process communication activity by the malware, the Sysmon log was filtered for `EventID 17, PipeEvent (CreatePipe)`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[
        System[(EventID=17)]
        and
        EventData[Data[@Name='ProcessId']='10672']
      ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:57`, PID `10672` created a named pipe referencing its own installation path:

- **PipeName**: `\ToServerAdvinst_Extract_C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe`

This behavior is consistent with installer inter-process communication during malicious payload extraction, but is not independently indicative of malicious lateral movement or process injection.

Additionally, there were no related `EventID 18, PipeEvent (PipeConnected)` events.

Payload Dropped to Disk

To identify the files dropped by the malware upon execution, the Sysmon log was again filtered for `EventID 11, FileCreate` and refined to include only events in which the creating image was the malicious installer.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[
        System[(EventID=11)]
        and
        EventData[Data[@Name='Image']='C:
\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe']
      ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:58`, the following files were written to the disk under `C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`:

- `c.cmd`
- `cmmc.cmd`
- `on.cmd`
- `once.cmd`
- `taskhost.exe`
- `viewer.exe`

Furthermore, `EventID 23, FileDelete` indicated the following files were written and subsequently deleted during the installation process:

File	Relation
`ddengine.dll`	UltraVNC component
`vnchooks.dll`	UltraVNC component
`UVncVirtualDisplay\UVncVirtualDisplay.dll`	UltraVNC virtual display driver
`powercfg.msi`	MSI package deleted post-extraction
`main1.msi`	MSI package deleted post-extraction

These deletions are indicative of a multi-stage MSI-based installer chain. Most notably, `msiexec.exe` ran as `NT AUTHORITY\SYSTEM` during the installation, indicating the installer requested and received elevated privileges during installation.

Though there are discrepancies between Unit42's threat intelligence documentation and the observed behavior during this compromise, that can be expected; still, these files are indicative of the trojanized UltraVNC malware. Through sandbox analysis, `taskhost.exe` is a renamed copy of the UltraVNC executable, `WinVNC.exe`. Furthermore, the `.cmd` scripts launch the VNC client and connect to the malicious server.

Timestomping

To gain a deeper understanding of the behavior of this malware and identify any additional malicious activity, the Sysmon log was filtered for `EventID 2, FileCreateTime`, which will return any events wherein the manipulation of file creation time metadata took place.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[
        System[(EventID=2)]
      ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:58`, under ProcessID `10672`, the malware modified the creation timestamp of the dropped decoy PDF file:

- **Target file**: `C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\~.pdf`
- **Original timestamp**: `2024-02-14 03:41:58`
- **Forged timestamp**: `2024-01-14 08:10:06`

This defense evasion technique is known as MITRE T1070.006 - Indicator Removal: Timestomp. It is commonly used to make malicious files appear unrelated to an attack with the intention of evading forensic timeline analysis.

File Deletion and Anti-Forensic Activity

To further identify file deletion and anti-forensic activity performed by the malware, the Sysmon log was filtered for `EventID 23, FileDelete`.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
      *[
        System[(EventID=23)]
        and
        EventData[Data[@Name='ProcessId']='10672']
      ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:57`, PID `10672` deleted several temporary executable files from `C:\Users\CyberJunkie\AppData\Local\Temp\`:

- `shiC46A.tmp`
- `MSIC49A.tmp`
- `MSIC4E9.tmp`
- `MSIC4FA.tmp`

This behavior is consistent with routine installer cleanup of temporary extraction files.

However, at `2024-02-14 03:41:58`, `once.cmd` was deleted with the `Archived` field recorded as `shredded file with pattern 0x74697865`. This is a nonstandard file deletion procedure and indicates the deliberate overwrite of file contents with a repeating byte pattern before deletion. This behavior is instead consistent with secure file-wiping techniques intended to prevent forensic recovery under MITRE T1485 - Data Destruction.

Process Termination

Finally, the Sysmon log was filtered for `EventID 5, ProcessTerminate` to identify when the malicious installer process terminated.

```
<QueryList>
  <Query Id="0" Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
    <Select Path="file://C:\[.]\Microsoft-Windows-Sysmon-Operational.evtx">
          *[
            System[(EventID=5)]
            and
            EventData[Data[@Name='ProcessId']='10672']
          ]
    </Select>
  </Query>
</QueryList>
```

At `2024-02-14 03:41:58`, ProcessID `10672` (`Preventivo24.02.14.exe.exe`) terminated after fully deploying the malicious payload to the disk.

Indicators of Compromise (IoCs)

Files

Name	Path	SHA256	Notes
`Preventivo24.02.14.exe.exe`	`C:\Users\CyberJunkie\Downloads\`	`0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3`	Trojanized UltraVNC installer, creates and sets specific registry keys
`Fattura 2 2024.exe`	-	-	`Preventivo24.02.14.exe.exe`'s original filename as identified by its embedded metadata

Name	Path	SHA256	Notes
`~.pdf`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\`	`01fa678a302763b83703f0449fc63309cf7677fc119d2755defad6dea9d25bcd`	Decoy PDF, timestomped
`taskhost.exe`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`3fb38eefb8db4d52be428facc8a242997ab2ad58a8d08980a7688c9bf0b30454`	Renamed instance of `WinVNC.exe`
`on.cmd`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`1ce4768f825372d55c1d30ce3ac41afb913de6299a64ae5b0ac1b3b752421d64`	Launches UltraVNC, establishes persistence via registry as per Unit42 analysis
`c.cmd`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`c2ab7b8701bdc36198a8f01791c8a3479ef3e8bcc6ccd3bd8c2f60dd9672e8e1`	Called by `on.cmd`
`cmmc.cmd`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`d69e739f18bd24db5cfd451fb2bdab32b4efeef41145b75cb89c7dc56641852d`	Observed in Sysmon logs, not documented by Unit42
`once.cmd`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`e596899f114b5162402325dfb31fdaa792fabed718628336cc7a35a24f38eaa9`	Securely shredded post-execution with pattern `0x74697865`
`viewer.exe`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`e48aac5148b261371c714b9e00268809832e4f82d23748e44f5cfbbf20ca3d3f`	Observed in Sysmon logs, not documented by Unit42
`ddengine.dll`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`0d44439a0425df8abf338bd1496679a144dd705a51832a05c1a4ed1f76756eba`	UltraVNC component, deleted post-installation

Name	Path	SHA256	Notes
`vnchooks.dll`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`4d12febd622266220aa2dd2074972ee82545c144dc599f68866212a29db9f442`	UltraVNC component, deleted post-installation
`UVncVirtualDisplay.dll`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\`	`ff9d8f7fc2c3f5d0afaf6f76e87d41feeabf54facbe26dc59661a78830f32972`	UltraVNC virtual display driver, deleted post-installation
`main1.msi`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\`	`b73b46f35142989a10c91aa887f94037271b8ee7148cc3bfb061ae9848ed1fd9`	MSI installer package, deleted post-extraction
`powercfg.msi`	`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	`c5bf02c8c23dbf8798d87fad91ea44a3153fc1026248bd931f360ba0d6c5989e`	MSI installer package, deleted post-extraction

Named Pipes

Pipe Name	Notes
`\ToServerAdvinst_Extract_C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe`	Created by PID `10672` during payload extraction; consistent with installer inter-process communication

Network

Type	Value	Notes
Dropbox delivery URL	`https://www.dropbox[.]com/`	ReferrerURL at download
Dropbox CDN	`https://uc2f030016253ec53f4953980a4e.dl.dropboxusercontent[.]com/cd/0/get/CNNlOCYTD8cqLXFQzXaeYHRkHg_PoR35Et2T0_IkqE5ijvkTAQNljV7ZkK2fLXWI2bJy944RnwKttvmNWpVd5olpBcffnvnL_IfEjzr65jZZUOxtWA9rSgJ1jc91IZILHVAJHgRhjpZYLtGo83_QbeInB7x2oEAoYg-JLF54zbhziQ/file`	HostURL at download
Connectivity check domain	`www.example[.]com`	Not explicitly malicious, connectivity check only
Connectivity check IP	`93.184.216[.]34:80`	Resolves to `www.example[.]com`

Type	Value	Notes
VNC C2 domain	`vnvariant2024.ddnsfree[.]com:5500`	Malicious VNC server, not captured in Sysmon log; Unit42 defined
VNC C2 IP	`140.228.29[.]110:5500`	Resolves to `vnvariant2024.ddnsfree[.]com:5500`
Compromised system source IP	`172.17.79[.]132:61177`	Outbound connection from `DESKTOP-887GK2L`

Registry

Key	Notes
`HKU\[SID]\Software\Microsoft\SystemCertificates\Root\Certificates`	Root certificate store key created by malware (T1553.004)
`HKU\[SID]\Software\Microsoft\SystemCertificates\CA\Certificates`	CA certificate store key created by malware (T1553.004)

Directory Artifact

Path	Notes
`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\`	Root malware installation directory, creation time aligns with infection
`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\`	Decoy PDF drop location
`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\`	Primary payload drop location of scripts, executables, and DLLs
`C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\`	UltraVNC virtual display driver location
`C:\Users\CyberJunkie\AppData\Local\Temp\`	Temporary installer extraction files, deleted post-installation
`C:\Windows\Installer\`	MSI installer staging directory used by `msiexec.exe` during elevated installation

Endpoints

Endpoint	Related User	Notes
`DESKTOP-887GK2L`	`CyberJunkie`	The only endpoint which evidence indicates as compromised

Users

User	Related Endpoint	Notes
`CyberJunkie`	`DESKTOP-887GK2L`	The only user which evidence indicates as compromised

Root Cause Analysis

Though the Sysmon logs do not provide a comprehensive overview of all related endpoint activity within the investigation timeframe, the Unit42 threat intelligence report for this malware campaign can be used as supplementary information.

The root cause of this incident can be assumed to be user interaction with a malicious file delivered via social engineering methods -- most likely phishing, as detailed within threat intelligence reports. User `CyberJunkie` downloaded `Preventivo24.02.14.exe.exe` from a Dropbox-hosted link, executing it shortly thereafter. The malware was a trojanized UltraVNC installer which, according to Unit42 threat intelligence, was disguised as a legitimate Italian business invoice.

- "Preventivo" translates to "Estimate" or "Quote" in Italian, which likely lowered user suspicion.

No explicit software vulnerabilities or misconfigurations were found to be exploited to achieve initial access, as the compromise relied solely on end-user interaction. Furthermore, the absence, lack of, or misconfiguration of Endpoint Detection and Response (EDR) capabilities on `DESKTOP-887GK2L` allowed the malware to execute, drop its payload to the disk, manipulate file timestamps and registry keys and values, and issue outbound network connections. Should there have been EDR capabilities on this system, these actions would have generated alerts and triggered automated responses.

Technical Timeline

The Sysmon log does not provide a comprehensive overview of all related endpoint, network, or environment activity within the investigation timeframe. Therefore, the following timeline components are included, but are affected by a gap in event visibility:

- Reconnaissance
- Enumeration
- Containment
- Eradication
- Recovery

Reconnaissance

No evidence of reconnaissance activity was identified in the Sysmon log or documented in Unit 42's threat intelligence report for this campaign.

Initial Compromise

Time	Activity
2024-02-14 03:31:26	Mozilla Firefox downloaded Preventivo24.02.14.exe.exe from a Dropbox-hosted URL to C:\Users\CyberJunkie\Downloads\
2024-02-14 03:41:26	Sysmon FileCreate event confirms Preventivo24.02.14.exe.exe was written to the disk
2024-02-14 03:41:56	Explorer.EXE deleted the Zone.Identifier Alternate Data Stream (ADS) from Preventivo24.02.14.exe.exe prior to execution (T1553.005)
2024-02-14 03:41:56	Preventivo24.02.14.exe.exe executed under ProcessID (PID) 10672; confirmed unsigned with original filename of Fattura 2 2024.exe

C2 Communications

Time	Activity
2024-02-14 03:41:56	PID 10672 issued a DNS query for www.example.com for a connectivity check
2024-02-14 03:41:57	PID 10672 established an outbound connection to 93.184.216[.]34:80 (www.example.com), confirming connectivity check
Unit42 documented, not captured in Sysmon log	VNC C2 channel established to vnvariant2024.ddnsfree[.]com:5500 (140.228.29[.]110)

Enumeration

No evidence of enumeration activity was identified in the Sysmon log or documented in Unit 42's threat intelligence report for this campaign.

Lateral Movement

No evidence of enumeration activity was identified in the Sysmon log or documented in Unit 42's threat intelligence report for this campaign. As no DNS queries were made laterally, this compromise appears to be isolated to DESKTOP-887GK2L.

Data Access and Exfiltration

No explicit evidence of data access or exfiltration was identified in the Sysmon log or documented in Unit 42's threat intelligence report for this campaign; however, the successful establishment of a VNC server and the addition of a root and CA certificate suggest a breach of data confidentiality related to any information found on CyberJunkie's screen from the point of infection.

Malware Deployment and Activity

Time	Activity
2024-02-14 03:41:56	PID 10672 loaded itself as a DLL, flagged by Sysmon as T1574.002 (DLL Side-Loading); loaded urlmon.dll for URL/download handling
2024-02-14 03:41:57	PID 10672 loaded .NET runtime DLLs mscoree.dll and mscoreei.dll, flagged by Sysmon as T1055.001 (Process Injection: Dynamic-link Library Injection); no CreateRemoteThread events confirmed

Time	Activity
2024-02-14 03:41:57	PID 10672 created named pipe \ToServerAdvinst_Extract_C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe consistent with installer extraction inter-process communication
2024-02-14 03:41:57	PID 10672 created registry keys in HKU\S-1-5-21-3393683511-3463148672-371912004-1001\Software\Microsoft\SystemCertificates\Root\Certificates and HKU\S-1-5-21-3393683511-3463148672-371912004-1001\Software\Microsoft\SystemCertificates\CA\Certificates (T1553.004)
2024-02-14 03:41:57	BAM registry value set for Preventivo24.02.14.exe.exe and msiexec.exe, forensically indicating execution
2024-02-14 03:41:57	PID 10672 deleted temporary installer files shiC46A.tmp, MSIC49A.tmp, MSIC4E9.tmp, MSIC4FA.tmp from AppData\Local\Temp\
2024-02-14 03:41:58	PID 10672 loaded taskschd.dll, flagged by Sysmon as T1053.005 (Scheduled Task/Job: Scheduled Task), possible persistence attempt; no ServiceStateChanged events identified
2024-02-14 03:41:58	Payload files dropped to C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\: c.cmd, cmmc.cmd, on.cmd, once.cmd, taskhost.exe, viewer.exe; additional UltraVNC components ddengine.dll, vnchooks.dll, UVncVirtualDisplay.dll written and deleted post-installation
2024-02-14 03:41:58	MSI packages main1.msi and powercfg.msi written and deleted; msiexec.exe executed as NT AUTHORITY\SYSTEM, indicating installer elevation during installation
2024-02-14 03:41:58	BAM registry value set for msiexec.exe, forensically indicating elevated privileges during installer activity
2024-02-14 03:41:58	Decoy PDF ~.pdf dropped to C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\; creation timestamp forged from 2024-02-14 03:41:58 to 2024-01-14 08:10:06 T1070.006 (Indicator Removal: Timestomp)
2024-02-14 03:41:58	once.cmd securely shredded with pattern 0x74697865 prior to deletion, indicating deliberate anti-forensic activity T1485 (Data Destruction)
2024-02-14 03:41:58	PID 10672 (Preventivo24.02.14.exe.exe) terminated; VNC payload left running independently
Per Unit 42 threat intelligence	on.cmd establishes persistence via registry run key; corresponding registry write not captured in Sysmon log

Process Injection

No EventID 8, CreateRemoteThread events were identified to directly conclude process injection. Sysmon flagged the loading of .NET runtime DLLs mscoree.dll and mscoreei.dll under PID 10672 as T1055.001 (Process Injection: Dynamic-link Library Injection); however, DLL loads alone are insufficient to conclude process injection without supplementary evidence.

Containment, Eradication, and Recovery

No evidence of containment, eradication, or recovery activity was identified in the Sysmon log.

Nature of the Attack

This incident follows behavior consistent with a trojanized UltraVNC remote access malware package. It was documented in Palo Alto's Unit42 Threat Intelligence report for this campaign as a socially engineered Italian malware-spam (malspam) delivery campaign active as early as January 22, 2024. This incident relied solely on user interaction rather than software exploitation or misconfiguration, and employed multiple defense evasion techniques to reduce the likelihood of detection and forensic analysis.

Delivery and Initial Access

The malware was delivered via a Dropbox-hosted link, which, according to Unit42's threat intelligence documentation, was likely distributed through a malicious email. The installer was disguised as a legitimate Italian business invoice under the filename `Preventivo24.02.14.exe.exe`, which translates roughly to "Estimate" or "Quote" in Italian. The executable's embedded metadata identified it as `Fattura 2 2024.exe`, translating to "Invoice 2 2024". The use of a double extension (T1036.007) and a common filename was likely intended to lower user suspicion and bypass initial file inspection and user insight. The file was also unsigned, which would have triggered `SmartScreen` or `User Account Control` (UAC) warnings on initial download; however, the `Zone.Identifier` Alternate Data Stream was removed by `Explorer.EXE` before execution (T1553.005), likely suppressing these protections.

Execution and Installation

Upon execution, the malware was installed through a multi-stage MSI-based package, which invoked `msiexec.exe` with elevated privileges under `NT AUTHORITY\SYSTEM` to extract and install the trojanized UltraVNC package. A named pipe was created during extraction for inter-process communication between installer components, but was never connected. The `.NET runtime` was initialized during execution, with Sysmon flagging the loading of `mscoree.dll` and `mscoreei.dll` as indicative of T1055.001; however, no CreateRemoteThread events were identified, suggesting no process injection activity. The Task Scheduler COM API, `taskschd.dll`, was also loaded and flagged as T1053.005, suggesting attempted scheduled task persistence, but no direct scheduled task creation events were captured in the Sysmon log, refuting this.

Defense Evasion

The malware employed several techniques to evade detection and disrupt forensic analysis. Certificate store registry keys were created in both the trusted root and Certificate Authority stores, flagged as T1553.004, which was likely to suppress TLS trust warnings during the active VNC session. The decoy PDF `~.pdf` was flagged timestomped as T1070.006, altering its creation date to approximately one month prior, likely to make it appear unrelated to the infection. Temporary installer files, DLLs, and scripts were deleted post-extraction and post-infection for forensic obfuscation. Additionally, `once.cmd` was securely shredded using the repeating byte pattern `0x74697865` rather than deleted by standard deletion procedures, indicating deliberate anti-forensic actions aligned with T1485.

Command and Control

The malware issued an HTTP connectivity check to `www.example[.]com:80` (`93.184.216[.]34`) to confirm network access. Though not present within the Sysmon logs, Unit42's threat intelligence documentation listed the true C2 channel, which was established via `TCP/VNC` to

`vnvariant2024.ddnsfree[.]com:5500` (`140.228.29[.]110`). This VNC session visually shared the screen of `DESKTOP-887GK2L` via `RFB` over a non-standard port, which is behavior consistent with a malicious attempt to hide C2 traffic.

MITRE ATT&CK TTPs

Technique ID	Name	Observed Behavior
`T1036.007`	Masquerading: Double File Extension	`Preventivo24.02.14.exe.exe` used double extension to disguise executable
`T1553.005`	Subvert Trust Controls: Mark-of-the-Web Bypass	`Zone.Identifier` stream removed by `Explorer.EXE` prior to execution
`T1574.002`	DLL Side-Loading	Malware loaded itself as a DLL at execution
`T1055.001`	Process Injection: Dynamic-link Library Injection	`.NET runtime` DLLs loaded and flagged by Sysmon; unconfirmed without CreateRemoteThread evidence
`T1053.005`	Scheduled Task/Job: Scheduled Task	`taskschd.dll` loaded and flagged by Sysmon; unconfirmed without direct task creation evidence
`T1553.004`	Subvert Trust Controls: Install Root Certificate	Registry keys created in trusted root and CA certificate stores
`T1071`	Application Layer Protocol	VNC used as C2 communication channel
`T1070.006`	Indicator Removal: Timestomp	Decoy PDF creation timestamp forged by approximately one month
`T1070`	Indicator Removal	Temporary installer files deleted post-extraction
`T1485`	Data Destruction	`once.cmd` securely shredded with repeating-byte pattern

A Appendix

A.1 Technical Timeline

Time	Activity
2024-02-14 03:31:26	Mozilla Firefox downloaded Preventivo24.02.14.exe.exe from a Dropbox-hosted URL to C:\Users\CyberJunkie\Downloads\
2024-02-14 03:41:26	Sysmon FileCreate event confirms Preventivo24.02.14.exe.exe was written to the disk
2024-02-14 03:41:56	Explorer.EXE deleted the Zone.Identifier Alternate Data Stream (ADS) from Preventivo24.02.14.exe.exe prior to execution (T1553.005)
2024-02-14 03:41:56	Preventivo24.02.14.exe.exe executed under ProcessID (PID) 10672; confirmed unsigned with original filename of Fattura 2 2024.exe
2024-02-14 03:41:56	PID 10672 issued a DNS query for www.example.com for a connectivity check
2024-02-14 03:41:57	PID 10672 established an outbound connection to 93.184.216[.]34:80 (www.example.com), confirming connectivity check
2024-02-14 03:41:56	PID 10672 loaded itself as a DLL, flagged by Sysmon as T1574.002 (DLL Side-Loading); loaded urlmon.dll for URL/download handling
2024-02-14 03:41:57	PID 10672 loaded .NET runtime DLLs mscoree.dll and mscoreei.dll, flagged by Sysmon as T1055.001 (Process Injection: Dynamic-link Library Injection); no CreateRemoteThread events confirmed
2024-02-14 03:41:57	PID 10672 created named pipe \ToServerAdvinst_Extract_C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe consistent with installer extraction inter-process communication
2024-02-14 03:41:57	PID 10672 created registry keys in HKU\S-1-5-21-3393683511-3463148672-371912004-1001\Software\Microsoft\SystemCertificates\Root\Certificates and HKU\S-1-5-21-3393683511-3463148672-371912004-1001\Software\Microsoft\SystemCertificates\CA\Certificates (T1553.004)
2024-02-14 03:41:57	BAM registry value set for Preventivo24.02.14.exe.exe and msiexec.exe, forensically indicating execution
2024-02-14 03:41:57	PID 10672 deleted temporary installer files shiC46A.tmp, MSIC49A.tmp, MSIC4E9.tmp, MSIC4FA.tmp from AppData\Local\Temp\
2024-02-14 03:41:58	PID 10672 loaded taskschd.dll, flagged by Sysmon as T1053.005 (Scheduled Task/Job: Scheduled Task), possible persistence attempt; no ServiceStateChanged events identified
2024-02-14 03:41:58	Payload files dropped to C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\: c.cmd, cmmc.cmd, on.cmd, once.cmd, taskhost.exe, viewer.exe; additional UltraVNC components dd engine.dll, vnchooks.dll, UVncVirtualDisplay.dll written and deleted post-installation

Time	Activity
`2024-02-14 03:41:58`	MSI packages `main1.msi` and `powercfg.msi` written and deleted; `msiexec.exe` executed as `NT AUTHORITY\SYSTEM`, indicating installer elevation during installation
`2024-02-14 03:41:58`	BAM registry value set for `msiexec.exe`, forensically indicating elevated privileges during installer activity
`2024-02-14 03:41:58`	Decoy PDF `~.pdf` dropped to `C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\`; creation timestamp forged from `2024-02-14 03:41:58` to `2024-01-14 08:10:06` T1070.006 (Indicator Removal: Timestomp)
`2024-02-14 03:41:58`	`once.cmd` securely shredded with pattern `0x74697865` prior to deletion, indicating deliberate anti-forensic activity (T1485)
`2024-02-14 03:41:58`	PID `10672` (`Preventivo24.02.14.exe.exe`) terminated; VNC payload left running independently
Unit42 documented, not captured in Sysmon log	`on.cmd` establishes persistence via registry run key; corresponding registry write not captured in Sysmon log
Unit42 documented, not captured in Sysmon log	VNC C2 channel established to `vnvariant2024.ddnsfree[.]com:5500` (`140.228.29[.]110`)

End of Report

This report was rendered
by SysReptor with
♥