Elastic Security uncovers BLISTER malware campaign

By Joe Desimone, Samir Bousseaden

Published: 2022-08-03 · Archived: 2026-04-06 01:26:40 UTC

Key takeaways:

- Elastic Security uncovered a stealthy malware campaign that leverages valid code signing certificates to evade detection
- A novel malware loader, BLISTER was used to execute second stage malware payloads in-memory and maintain persistence
- The identified malware samples have very low or no detections on VirusTotal
- Elastic provided layered prevention coverage from this threat out of the box

> For information on the BLISTER malware loader and campaign observations, check out our blog post and configuration extractor detailing this:
>
> - BLISTER Malware Analysis
> - BLISTER Configuration Extractor

Overview

The Elastic Security team identified a noteworthy cluster of malicious activity after reviewing our threat prevention telemetry. A valid code signing certificate is used to sign malware to help the attackers remain under the radar of the security community. We also discovered a novel malware loader used in the campaign, which we've named BLISTER. The majority of the malware samples observed have very low, or no, detections in

Elastic's layered approach to preventing attacks protects from this and similar threats.

In one prevented attack, our malicious behavior prevention triggered multiple high-confidence alerts for *Execution via Renamed Signed Binary Proxy*, *Windows Error Manager/Reporting Masquerading*, and *Suspicious PowerShell Execution via Windows Scripts*. Further, our memory threat prevention identified and stopped BLISTER from injecting its embedded payload to target processes.

Finally, we have additional coverage from our open source detection engine rules [

Details

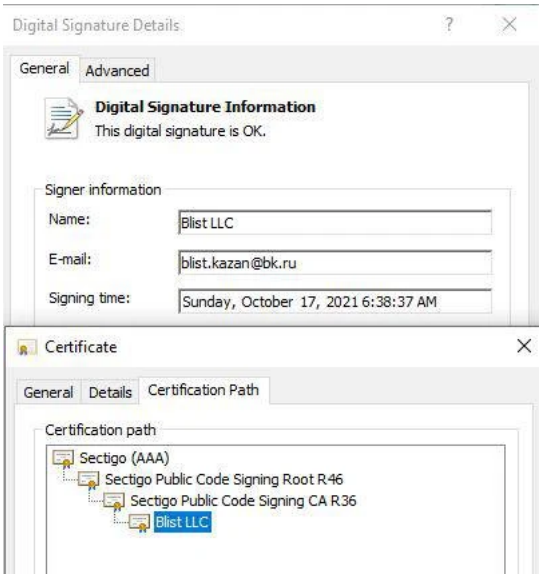
Certificate abuse

A key aspect of this campaign is the use of a valid code signing certificate issued by

We responsibly disclosed the activity to Sectigo so they could take action and revoke the abused certificates. Below shows details about the compromised certificate. We have observed malware signed with this certificate as early as September 15, 2021.

Issuer: *Sectigo Public Code Signing CA R36_Issued to: _Blist LLC_Serial number: _2f4a25d52b16eb4c9dfe71ebbd8121bb_Valid from: _Monday, August 23, 2021 4:00:00 PM_Valid to: _Wednesday, August 24, 2022 3:59:59 PM*

VirusTotal. The infection vector and goals of the attackers remain unknown at this time.1] [2]. To ensure coverage for the entire community, we are including YARA rules and IoCs to help defenders identify impacted systems.Sectigo. Adversaries can either steal legitimate code-signing certificates or purchase them from a certificate authority directly or through front companies. Executables with valid code signing certificates are often scrutinized to a lesser degree than unsigned executables. Their use allows attackers to remain under the radar and evade detection for a longer period of time.

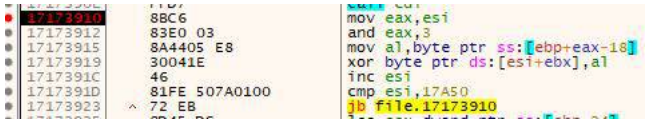


BLISTER malware loader

Another interesting aspect of this campaign is what appears to be a novel malware loader with limited detections in VirusTotal. We refer to it as the BLISTER loader. The loader is spliced into legitimate libraries such as colorui.dll, likely to ensure the majority of the on-disk footprint has known-good code and metadata. The loader can be initially written to disk from simple dropper executables. One such dropper writes a signed BLISTER loader to *%temp%\Framwork\axsssig.dll* and executes it with *rundll32*. *LaunchColorCpl* is a common DLL export and entry point name used by BLISTER as seen in the command line parameters:

```
Rundll32.exe C:\Users\user\AppData\Local\Temp\Framwork\axsssig.dll,LaunchColorCpl
```

Once executed, BLISTER decodes bootstrapping code stored in the resource section with a simple 4-byte XOR routine shown below:



The bootstrapping code is heavily obfuscated and initially sleeps for 10 minutes. This is likely an attempt to evade sandbox analysis. After the delay, it decrypts the embedded malware payload. We have observed CobaltStrike and BitRat as embedded malware payloads. Once decrypted, the embedded payload is loaded into the current process or injected into a newly spawned *WerFault.exe* process.

Finally, BLISTER establishes persistence by copying itself to the *C:\ProgramData* folder, along with a re-named local copy of *rundll32.exe*. A link is created in the current user's Startup folder to launch the malware at logon as a child of *explorer.exe*.

YARA

We have created a YARA rule to identify this BLISTER activity:

```
rule Windows_Trojan_Blister{
   meta:
       author = "Elastic Security"
       creation_date = "2021-12-20"
       last_modified = "2021-12-20"
       os = "Windows"
       category_type = "Trojan"
       family = "Blister"
       threat_name = "Windows.Trojan.Blister"
       reference_sample = "0a7778cf6f9a1bd894e89f282f2e40f9d6c9cd4b72be97328e681fe32a1b1a00"

   strings:
       $a1 = {8D 45 DC 89 5D EC 50 6A 04 8D 45 F0 50 8D 45 EC 50 6A FF FF D7}
       $a2 = {75 F7 39 4D FC 0F 85 F3 00 00 00 64 A1 30 00 00 00 53 57 89 75}
```

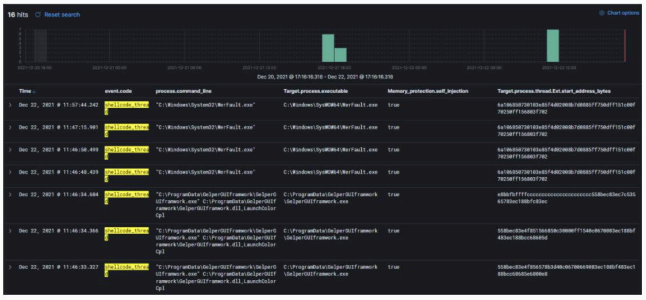
```
condition:
        any of them
}
```

Defensive recommendations

Elastic Endpoint Alerts

Elastic Endpoint Security provides deep coverage for this threat by stopping the in-memory thread execution and preventing malicious behaviors.

Memory Threat Detection Alert: Shellcode Injection



Malicious Behavior Detection Alert: Execution via Renamed Signed Binary Proxy

Hunting queries

These queries can be used in Kibana's Security -\> Timelines -\> Create new timeline -\> Correlation query editor. While these queries will identify this intrusion set, they can also identify other events of note that, once investigated, could lead to other malicious activities.

Proxy Execution via Renamed Rundll32

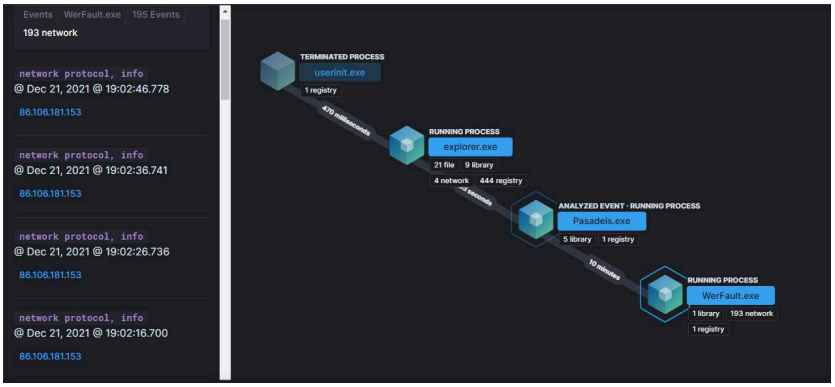
Hunt for renamed instances of *rundll32.exe*

```
 process where event.action == "start" and
process.name != null and
(process.pe.original_file_name == "RUNDLL32.EXE" and not process.name : "RUNDLL32.EXE")
```

Masquerading as WerFault

Hunt for potential rogue instances of WerFault.exe (Windows Errors Reporting) in an attempt to masquerade as a legitimate system process that is often excluded from behavior-based detection as a known frequent false positive:

```
process where event.action == "start" and
 process.executable :
  ("?:\\Windows\\Syswow64\\WerFault.exe" ,"?:\\Windows\\System32\\WerFault.exe") and
  /*
    legit WerFault will have more than one argument in process.command_line
  */
 process.args_count == 1
```



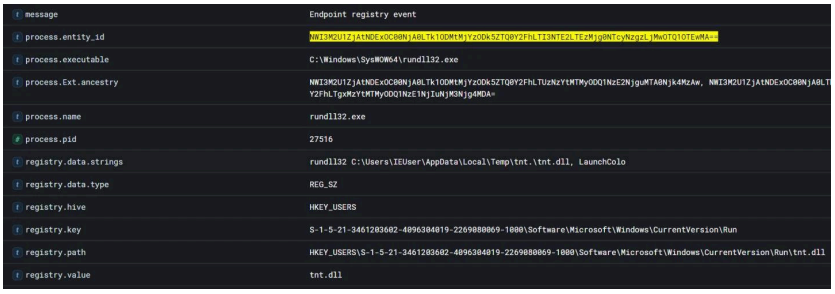
Evasion via Masquerading as WerFault and Renamed Rundll32

Persistence via Registry Run Keys / Startup Folder

Malware creates a new run key for persistence:

```
registry where registry.data.strings != null and
registry.path : (
 /* Machine Hive */      "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\*",
"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run\\*",  "HKLM\\Software\\Microsoft\\Windows NT\

 /* Users Hive */
"HKEY_USERS\\*\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\*",
"HKEY_USERS\\*\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\Run\\*", "HKEY_USERS\\*\\Software\\Micro
    )
```

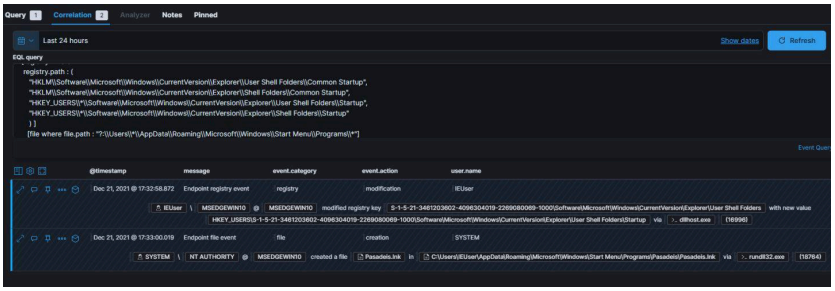


Persistence via Run key

Suspicious Startup Shell Folder Modification

Modify the default Startup value in the registry via COM (dllhost.exe) and then write a shortcut file for persistence in the new modified Startup folder:

```
sequence by host.id with maxspan=1m
[registry where
 /* Modify User default Startup Folder */
 registry.path : (
    "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders\\Common Startup",
    "HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell Folders\\Common Startup",
    "HKEY_USERS\\*\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell Folders\\Startup",
    "HKEY_USERS\\*\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell Folders\\Startup"
    ) ]
 /* Write File to Modified Startup Folder */
   [file where event.type : ("creation", "change") and file.path : "?:\\Users\\*\\AppData\\Roaming\\Microsoft\\Windows\\S
```



Persistence via Modified Startup

Elastic Detection Engine Rules

The following existing public detection rules can also be used to detect some of the employed techniques:

Potential Windows Error Manager Masquerading

Windows Defender Exclusions Added via PowerShell

Startup or Run Key Registry Modification

Shortcut File Written or Modified for Persistence

Suspicious Startup Shell Folder Modification

MITRE ATT&CK

T1218.011 - Signed Binary Proxy Execution: Rundll32

T1055 - Process Injection

T1547.001 - Registry Run Keys / Startup Folder

T1036 - Masquerading

Summary

The BLISTER loader has several tricks which has allowed it to fly under the radar of the security community for months. This includes leveraging valid code signing certificates, infecting legitimate libraries to fool machine learning models, and executing payloads in-memory. However, the depth of protection offered with Elastic Security meant we were still able to identify and stop in-the-wild attacks.

Existing Elastic Security can access these capabilities within the product. If you're new to Elastic Security, take a look at our Quick Start guides (bite-sized training videos to get you started quickly) or our free fundamentals training courses. You can always get started with a free 14-day trial of Elastic Cloud.

Indicators

| | |

Indicator
F3503970C2B5D57687EC9E31BB232A76B624C838
moduleloader.s3.eu-west-2.amazonaws[.]comdiscountshadesdirect[].com bimelectrical[.]comclippershipintl[.]com
188.68.221[.]20393.115.18[.]24852.95.148[.]16284.38.183[.]17480.249.145[.]212185.170.213[.]186
ed6910fd51d6373065a2f1d3580ad645f443bf0badc398aa77185324b0284db8 cb949ebe87c55c0ba6cf0525161e2e6670c1ae186ab83ce46047446e9753a9
df8142e5cf897af65972041024ebe74c7915df0e18c6364c5fb9b2943426ed1a2d049f7658a8dccd930f7010b32ed1bc9a5cc0f8109b511ca2a77a210430136

Indicator
afb77617a4ca637614c429440c78da438e190dd1ca24dc78483aa731d80832c2516cac58a6bfec5b9c214b6bba0b724961148199d32fb42c01b12ac31f6a60
Launcher V7.3.13.exeGuiFramwork.exeffxivsetup.exePredictor V8.21 - Copy.exePredictor Release v5.9.rarPredictorGUI.exeReadhelper.exedxpo8umrz
Holorui.dllColorui.dllPasade.dllAxsssig.dllHelper.CC.dllHeav.dllPasadeis.dllTermmgr.dllTermService.dllrdpencom.dlllibcef.dlltnt.dll

---

Source: https://www.elastic.co/blog/elastic-security-uncovers-blister-malware-campaign