

# BLISTER malware campaign discovered | Elastic Blog

[elastic.co/blog/elastic-security-uncovers-blister-malware-campaign](https://elastic.co/blog/elastic-security-uncovers-blister-malware-campaign)



## 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

## 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 VirusTotal. The infection vector and goals of the attackers remain unknown at this time.

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 [1] [2]. To ensure coverage for the entire community, we are including YARA rules and IoCs to help defenders identify impacted systems.

## Details

---

### Certificate abuse

---

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

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*

General

Advanced

**Digital Signature Information**

This digital signature is OK.

## Signer information

Name:

Blist LLC

E-mail:

blist.kazan@bk.ru

Signing time:

Sunday, October 17, 2021 6:38:37 AM



## Certificate



General

Details

Certification Path

## Certification path



Sectigo (AAA)



Sectigo Public Code Signing Root R.46



Sectigo Public Code Signing CA R.36



Blist LLC

**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:

17173910	8BC6	mov eax,esi
17173912	83E0 03	and eax,3
17173915	8A4405 E8	mov al,byte ptr ss:[ebp+eax-18]
17173919	30041E	xor byte ptr ds:[esi+ebx],al
1717391C	46	inc esi
1717391D	81FE 507A0100	cmp esi,17A50
17173923	72 EB	jb file.17173910

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 renamed 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}

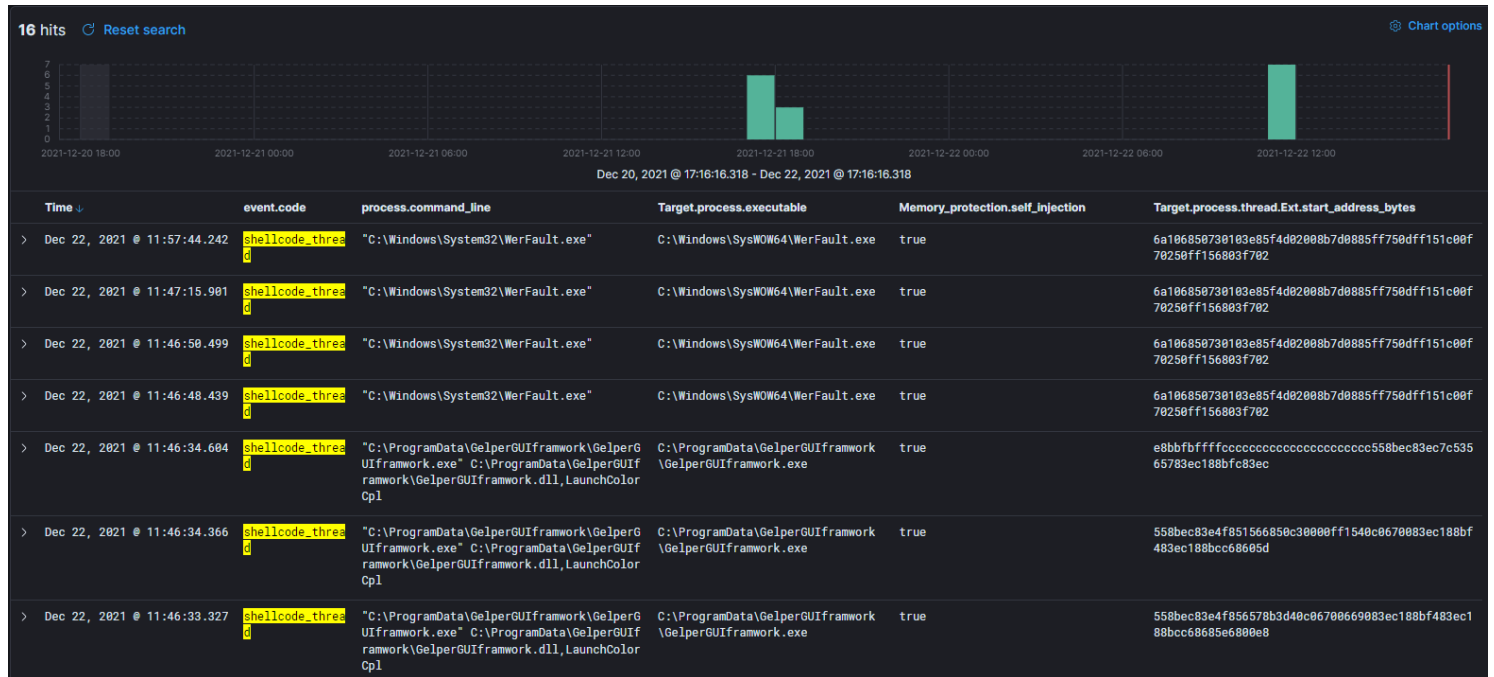
  condition:
    any of them
}Read more
```

## Defensive recommendations

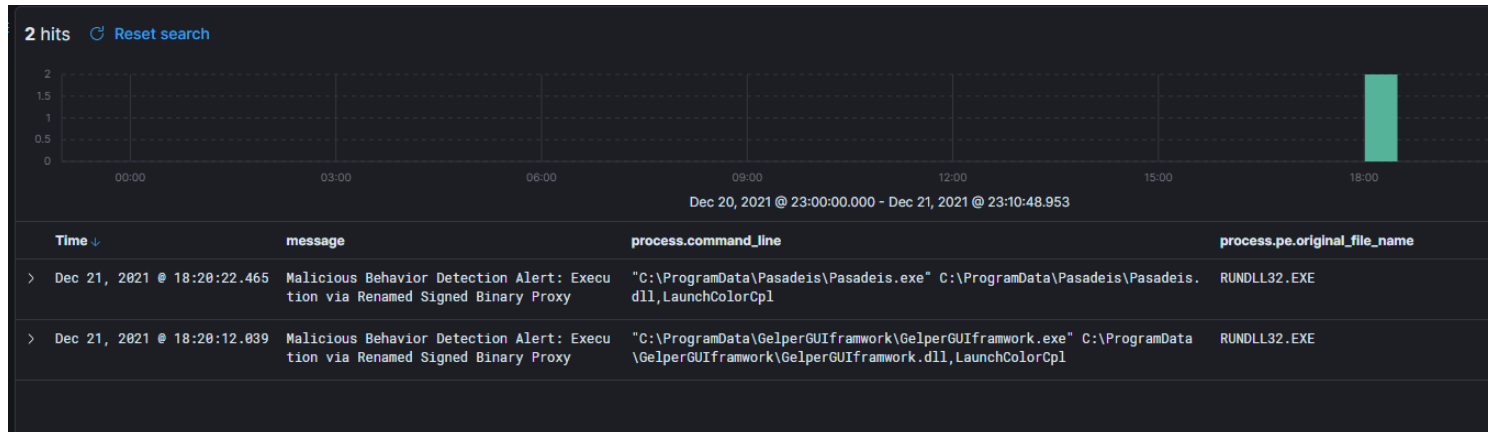
### Elastic Endpoint Alerts

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

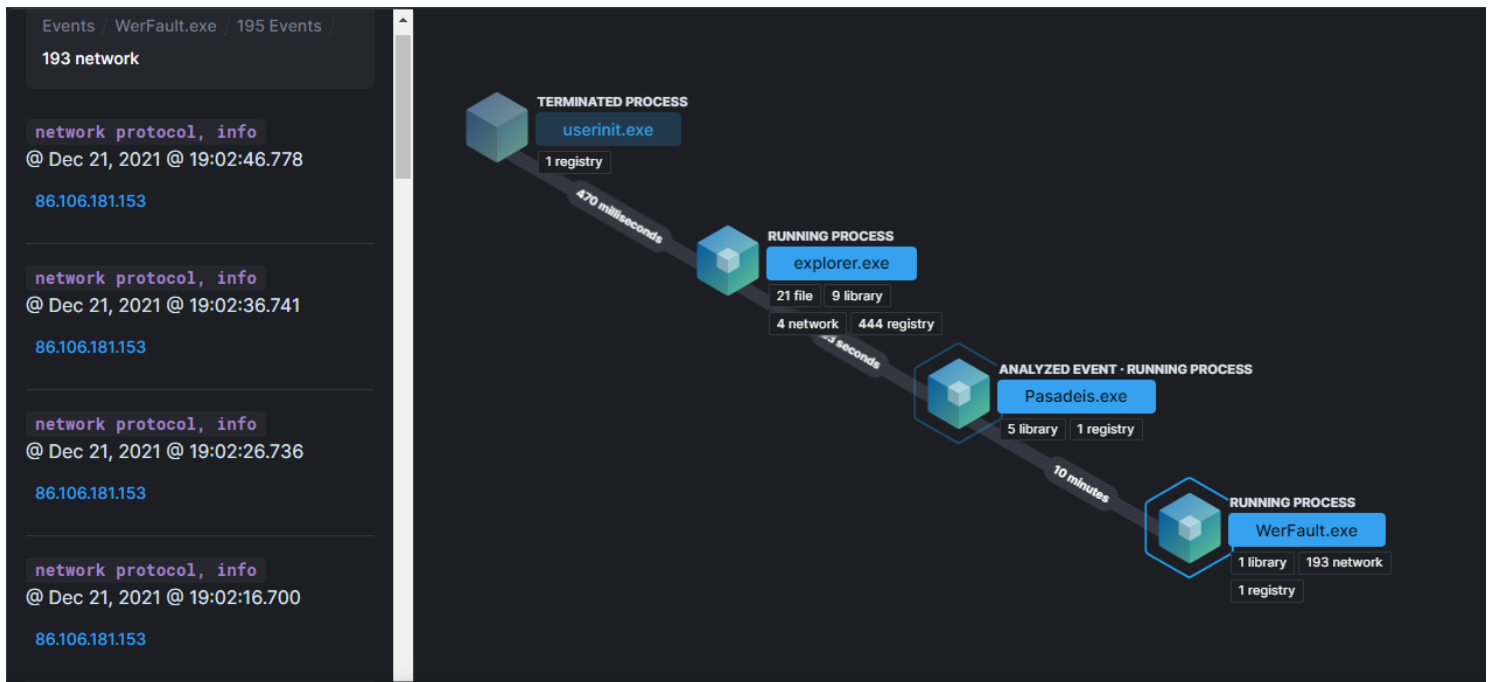
Hunt for renamed instances of *rundll32.exe*

```
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")
/*
  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\\CurrentVersion\\Winlogon\\Shell\\*",

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

message	Endpoint registry event
process.entity_id	NWI3M2U1ZjAtNDExOC08NjA0LTk1ODMtMjYzODk5ZTQ8Y2FhLTU3NTE2LzEzMjg8NTcyNzgzLjMwOTQ1OTUwMA==
process.executable	C:\Windows\SysWOW64\rundll32.exe
process.Ext.ancestry	NWI3M2U1ZjAtNDExOC08NjA0LTk1ODMtMjYzODk5ZTQ8Y2FhLTUzNzYtMTMyODQ1NzE2NjguMTA8Njk4MzAw, NWI3M2U1ZjAtNDExOC08NjA0LTU3NTE2LzEzMjg8NTcyNzgzLjMwOTQ1OTUwMA=
process.name	rundll32.exe
process.pid	27516
registry.data.strings	rundll32 C:\Users\IEUser\AppData\Local\Temp\tnt.\tnt.dll, LaunchColor
registry.data.type	REG_SZ
registry.hive	HKEY_USERS
registry.key	S-1-5-21-3461203602-4096304019-2269080069-1000\Software\Microsoft\Windows\CurrentVersion\Run
registry.path	HKEY_USERS\S-1-5-21-3461203602-4096304019-2269080069-1000\Software\Microsoft\Windows\CurrentVersion\Run\tnt.dll
registry.value	tnt.dll

### 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\Start Menu\Programs\*"]
```

The screenshot displays a security tool interface with the following components:

- Query Bar:** Shows tabs for Query, Correlation, Analyzer, Notes, and Pinned. The current view is 'Correlation' for the last 24 hours.
- EQL Query:**

```
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"
) ]
[file where file.path : "?:\Users\*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\*"]
```
- Event List:**
  - Event 1:** Dec 21, 2021 @ 17:32:58.872. Endpoint registry event. Category: registry. Action: modification. User: IEUser. Details: Modified registry key S-1-5-21-3461203602-4096304019-2269080069-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders with new value HKEY\_USERS\S-1-5-21-3461203602-4096304019-2269080069-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup via >.dllhost.exe (16996).
  - Event 2:** Dec 21, 2021 @ 17:33:00.019. Endpoint file event. Category: file. Action: creation. User: SYSTEM. Details: Created a file Pasadels.lnk in C:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Pasadels.lnk via >.rundll32.exe (18764).

### 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	Type	Note
F3503970C2B5D57687EC9E31BB232A76B624C838	SHA1	Code-signing certificate thumbprint

---



---

moduleloader.s3.eu-west-2.amazonaws.com  
discountshadesdirect.com  
bimelectrical.com  
clippershipintl.com

Domain  
name Malware  
c2c

---

188.68.221.203  
93.115.18.248  
52.95.148.162  
84.38.183.174  
80.249.145.212  
185.170.213.186

IP  
Address Malware  
c2

---

ed6910fd51d6373065a2f1d3580ad645f443bf0badc398aa77185324b0284db8  
cb949ebe87c55c0ba6cf0525161e2e6670c1ae186ab83ce46047446e9753a926  
7b9091c41525f1721b12dcef601117737ea990cee17a8eecf81dcfb25ccb5a8f  
84a67f191a93ee827c4829498d2cb1d27bdd9e47e136dc6652a5414dab440b74  
cc31c124fc39025f5c3a410ed4108a56bb7c6e90b5819167a06800d02ef1f028  
9472d4cb393256a62a466f6601014e5cb04a71f115499c320dc615245c7594d4  
4fe551bcea5e07879ec84a7f1cea1036cfd0a3b03151403542cab6bd8541f8e5  
1a10a07413115c254cb7a5c4f63ff525e64adfe8bb60acef946bb7656b7a2b3d  
9bccc1862e3e5a6c89524f2d76144d121d0ee95b1b8ba5d0ffcaa23025318a60  
8a414a40419e32282d33af3273ff73a596a7ac8738e9cdca6e7db0e41c1a7658  
923b2f90749da76b997e1c7870ae3402aba875fdbdd64f79cbeba2f928884129  
ed241c92f9bc969a160da2c4c0b006581fa54f9615646dd46467d24fe5526c7a  
294c710f4074b37ade714c83b6b7bf722a46aef61c02ba6543de5d59edc97b60

sha256 Signed  
Droppers

---

df8142e5cf897af65972041024ebe74c7915df0e18c6364c5fb9b2943426ed1a2d049f7658a8dccc930f7010b32ed1bc9a5cc0f8109b511ca2a77a2104301369696f6274af4b9e8db4727269d43c83c350694bd1ef4bd5ccdc0806b1f014568aa34821b50aadee0dd85c382c43f44dae1e5fef0feb2f7aed6abf3f3e21f79947cd03b30cfeea07b5ea4c8976e6456cb65e09f6b8e7dcc68884379925681b1c481edf3a3b295b0189e54f79387e7df61250cc8eab4f1e8f42eb5042102df8f1f44e5770751679f178f90ef7bd57e8e4ccfb6051767d8e906708c52184bf27f320a7778cf6f9a1bd894e89f282f2e40f9d6c9cd4b72be97328e681fe32a1b1a00a486e836026e184f7d3f30eaa4308e2f0c381c070af1f525118a484a987827c1359ffa33784cb357ddabc42be1dcb9854ddb113fd8d6caf3bf0391380f9d640a863228efa55b54a8d03a87bb602a2e418856e0028ae409357454a6303b128224d0f934fd5d63a1524616bc13b51ce274539a8ead9b072e7f7fe1a14bb8b927a6c0f3b27ae4f7db457a86a38244225cca35aa0960eb6a685ed350e99a36c32b61216cb4f2caef59f297f72f7f271b084637e5087d59411ac77ddd3b87e7a90aa00eb2f75822abeb2e222d007bdec464bfbc3934b8be12983cc898b37c6ace08125a0d6a839c4dc708dcd1ef9395570cc86d54d4725b7daf56964017f66be3c13c7480998ade344b74e956f7d3a3f1a989aaf43446163a62f0a8ed34b0c010d05651e8a8e6f9c63c4c1162efadfc4cdd9ad634c5e00a5ab03259fcdeaa225acba3a50930e7a144637faf88a98f2990a27532bfd20a93dc160eb2db4fbc17b58fa885e9ea1293552cb45a89e740426fa9c313225ff77ad1980dfea83b6c4a91cbee3210360c5d0939c5d38b7b9f0c232cf9fbf93b46a19e53930a1606bda28a556ca9ea3f7870561ed3c6387daf495404ed3827f212472501d2541d5ccf8b941c61d2ba1e001c137533cd7fb6b38fe71fee489d61dbcfea45c37c5ec1bcf845c17ea84d547e97a030d2b02ac2eaa9763ffb4f96f6c54659533a23e17268aababca09d9cd2f3cfcc06b33eff91d55602cb33a66ab3fd4f540b9212f5ddae54a6c6f808f9b19e1fab1c1b83dc99386f0ceee8593ddfd461ac047eae812df8733	sha256	Unsigned BLISTER Loader DLL
--	--------	--------------------------------------

---

afb77617a4ca637614c429440c78da438e190dd1ca24dc78483aa731d80832c2516cac58a6bfec5b9c214b6bba0b724961148199d32fb42c01b12ac31f6a60998ae2c205220c95f0f7e1f67030a9027822cc18e941b669e2a52a5dbb5af74bc9fe7357d48906b68f094a81d19cc0ff93f56cc40454ac5f00e2e2d9c8ccdbc388af555d61becfcf0c13d4bc8ea7ab97dcdc6591f8c6bb892290898d28ebce1c5d96bf7bd5f405d3b4c9a71bcd1060395f28f2466fdb91cafc6e261a31d41eb37af5104d0ead2f178711b1e23db3c16846de7d1a3ac04dbe09bacebb847775d76d8e22cf159345852be585bc5a8e9af476b00bc91cdda98fd6a3244219a90ac9d9d54dfedda0efa36ed445d501845b61ab73c2102786be710ac19f697fc8d4ca5c	sha256	Signed BLISTER Loader DLL
--	--------	------------------------------------

---

---

	File name	Dropper Names
Launcher V7.3.13.exe		
GuiFramwork.exe		
ffxivsetup.exe		
Predictor V8.21 - Copy.exe		
Predictor Release v5.9.rar		
PredictorGUI.exe		
Readhelper.exe		
dxpo8umrzrr1w6gm.exe		
Pers.exe		
razer.exe		
Amlidiag.exe		
Modern.exe		
iuyi.exe		
Cleandevicelhelper.exe		
installer.exe		

---

	File name	BLISTER DLL Names
Holorui.dll		
Colorui.dll		
Pasade.dll		
Axsssig.dll		
Helper.CC.dll		
Heav.dll		
Pasadeis.dll		
Termmgr.dll		
TermService.dll		
rdpencom.dll		
libcef.dll		
tnt.dll		