Endpoint Protection - Symantec Enterprise

Archived: 2026-04-05 23:16:22 UTC

Organizations in 31 countries have been targeted in a new wave of attacks which has been underway since at least October 2016. The attackers used compromised websites or “watering holes” to infect pre-selected targets with previously unknown malware. There has been no evidence found yet that funds have been stolen from any infected banks.

The attacks came to light when a bank in Poland discovered previously unknown malware running on a number of its computers. The bank then shared indicators of compromise (IOCs) with other institutions and a number of other institutions confirmed that they too had been compromised.

As reported, the source of the attack appears to have been the website of the Polish financial regulator. The attackers compromised the website to redirect visitors to an exploit kit which attempted to install malware on selected targets.

Symantec has blocked attempts to infect customers in Poland, Mexico and Uruguay by the same exploit kit that infected the Polish banks. Since October, 14 attacks against computers in Mexico were blocked, 11 against computers in Uruguay, and two against computers in Poland.

Custom exploit kit

The attackers appear to be using compromised websites to redirect visitors to a customized exploit kit, which is preconfigured to only infect visitors from approximately 150 different IP addresses. These IP addresses belong to 104 different organizations located in 31 different countries. The vast majority of these organizations are banks, with a small number of telecoms and internet firms also on the list.

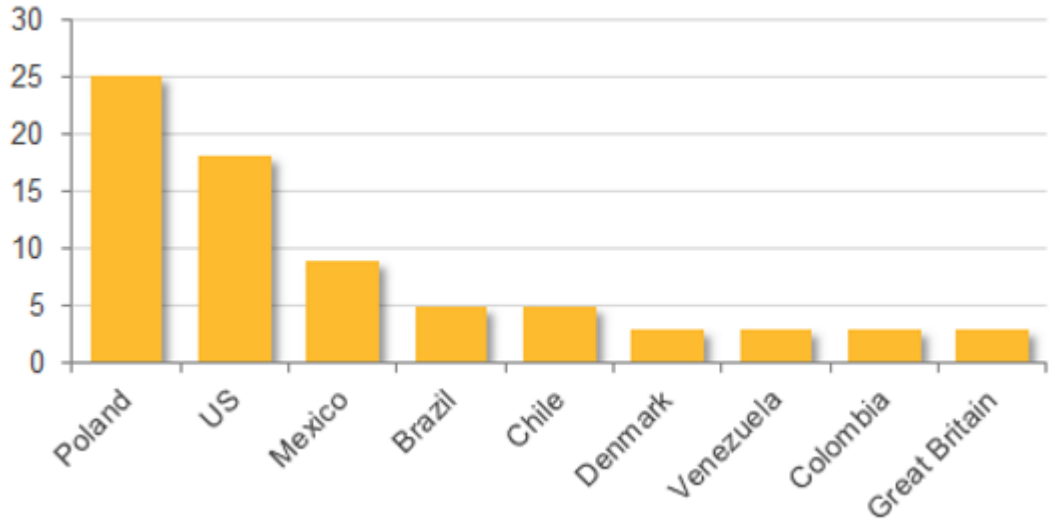

Figure 1. Countries in which three or more organizations were targeted by attackers

Links to Lazarus?

The malware used in the attacks (Downloader.Ratankba) was previously unidentified, although it was detected by Symantec under generic detection signatures, which are designed to block any files seen to engage in malicious activities.

Analysis of the malware is still underway. Some code strings seen in the malware used shares commonalities with code from malware used by the threat group known as Lazarus.

Ratankba was observed contacting eye-watch[.]in for command and control (C&C) communications.
Ratankba was then observed downloading a Hacktool. This Hacktool shows distinctive characteristics shared with malware previously associated with Lazarus.

```
data:0040B2CC ; char a_2fachi224A_q8[]
data:0040B2CC a_2fachi224A_q8 db '!_2FAcHI224$A_q8gS0dK',0 ; DATA XREF: sub_401E91+FD
data:0040B2E2                 align 4
data:0040B2E4 ; char aVwbebxyx1nzrck[]
data:0040B2E4 aVwbebxyx1nzrck db '!VWBeBxYx1nzrCkBLGQO',0 ; DATA XREF: sub_401E91+E7↑
data:0040B2F9                 align 4
data:0040B2FC ; char aUra9t1tcdes197[]
data:0040B2FC aUra9t1tcdes197 db '!uRa9t1tCDeS197CPt7I',0 ; DATA XREF: sub_401E91+D6↑
data:0040B311                 align 4
data:0040B314 ; char aEmcfgv7xc8itav[]
data:0040B314 aEmcfgv7xc8itav db '!emCFgv7Xc8ItaVGN0bMF',0 ; DATA XREF: sub_401E91+BC
data:0040B32A                 align 4
data:0040B32C ; char aIamsorry[]
data:0040B32C aIamsorry@12345 db 'iamsorry!@1234567',0 ; DATA XREF: sub_401E91+B1↑o
data:0040B33E                 align 10h
data:0040B340 ; char aInternetcloseh[]
data:0040B340 aInternetcloseh db 'InternetCloseHandle',0 ; DATA XREF: sub_401E91+A4↑o
data:0040B354 ; char aInternetreadfi[]
data:0040B354 aInternetreadfi db 'InternetReadFile',0 ; DATA XREF: sub_401E91+97↑o
data:0040B365                 align 4
data:0040B368 ; char aInternetcracku[]
data:0040B368 aInternetcracku db 'InternetCrackUrlA',0 ; DATA XREF: sub_401E91+8A↑o
data:0040B37A                 align 4
```

Figure 2. Code strings seen in sample of Hacktool used in recent attacks

```
.data:0040E27C ; char a_2fachi224A_q8[]
.data:0040E27C a_2fachi224A_q8 db '!_2FAcHI224$A_q8gS0dK',0 ; DATA XREF: sub_401362+FD
.data:0040E292                 align 4
.data:0040E294 ; char aVwbebxyx1nzrck[]
.data:0040E294 aVwbebxyx1nzrck db '!VWBeBxYx1nzrCkBLGQO',0 ; DATA XREF: sub_401362+E7↑
.data:0040E2A9                 align 4
.data:0040E2AC ; char aUra9t1tcdes197[]
.data:0040E2AC aUra9t1tcdes197 db '!uRa9t1tCDeS197CPt7I',0 ; DATA XREF: sub_401362+D6↑
.data:0040E2C1                 align 4
.data:0040E2C4 ; char aEmcfgv7xc8itav[]
.data:0040E2C4 aEmcfgv7xc8itav db '!emCFgv7Xc8ItaVGN0bMF',0 ; DATA XREF: sub_401362+BC
.data:0040E2DA                 align 4
.data:0040E2DC ; char aIamsorry[]
.data:0040E2DC aIamsorry@12345 db 'iamsorry!@1234567',0 ; DATA XREF: sub_401362+B1↑o
.data:0040E2EE                 align 10h
.data:0040E2F0 ; char aInternetcloseh[]
.data:0040E2F0 aInternetcloseh db 'InternetCloseHandle',0 ; DATA XREF: sub_401362+A4↑o
.data:0040E304 ; char aInternetreadfi[]
.data:0040E304 aInternetreadfi db 'InternetReadFile',0 ; DATA XREF: sub_401362+97↑o
.data:0040E315                 align 4
.data:0040E318 ; char aInternetcracku[]
.data:0040E318 aInternetcracku db 'InternetCrackUrlA',0 ; DATA XREF: sub_401362+8A↑o
```

Figure 3. Code strings seen in sample of Hacktool previously associated with Lazarus

Lazarus has been linked to a string of aggressive attacks since 2009, largely focused on targets in the US and South Korea. Lazarus has been involved in high level financial attacks before and some of the tools used in the Bangladesh bank heist shared code similarities with malware used in historic attacks linked to the group.

Further investigation of these attacks is underway and, over time, more evidence may emerge about the identity and motives of the attackers. After a series of high profile attacks on banks during 2016, this latest incident provides a timely reminder of the growing range of threats facing financial institutions.

[click_to_tweet:1]

UPDATE – March 15, 2017:

Further investigation by Symantec into the recent attacks against banks in Poland has uncovered additional links to the threat group known as Lazarus. At the time of our original blog, Symantec had found one link: code strings seen in a Hacktool used in the Polish bank attacks shared distinctive characteristics with malware previously associated with Lazarus.

The number of tentative links Symantec has established has since broadened from one to four. One piece of malware (MD5:91b2558f5319960c85522dc8e372a2b9) found on a computer at one of the Polish targets has been previously used and attributed to the Lazarus group. The previously mentioned Lazarus-linked Hacktool was also found on the same computer at the Polish target.

In addition to this, a sample of Downloader.Ratankba (MD5:cb52c013f7af0219d45953bae663c9a2), which has only been seen in the 2017 Polish Bank attacks, was submitted by a Symantec customer for analysis along with a sample of Backdoor.Destover, the disk-wiping malware linked to Lazarus and used in the Sony Pictures attacks.

A fourth link is the unique trait "del /a %1", which was found in Downloader.Ratankba. It was also identified in multiple malware families linked to Lazarus including Backdoor.Joanap and Backdoor.Destover.

As a result of these findings, Symantec has upgraded its assessment of a Lazarus link. The crossover in tools used leads us to believe there is a reasonable possibility that the Polish bank attacks were the work of attackers linked to Lazarus.

Protection

Symantec and Norton products protect against these attacks with the following detections:

- Downloader.Ratankba
- Web Attack: SunDown Exploit Kit Website 5
- Backdoor.Destover

IOCs

The follow are indicators of compromise related to these attacks.

Command and control infrastructure

- eye-watch[.]in
- sap.misapor[.]ch

Downloader.Ratankba

MD5

- 1f7897b041a812f96f1925138ea38c46
- 911de8d67af652a87415f8c0a30688b2
- 1507e7a741367745425e0530e23768e6
- cb52c013f7af0219d45953bae663c9a2
- 18a451d70f96a1335623b385f0993bcc

SHA256

- 99017270f0af0e499cfeb19409020bfa0c2de741e5b32b9f6a01c34fe13fda7d
- 825624d8a93c88a811262bd32cc51e19538c5d65f6f9137e30e72c5de4f044cc
- 200c0f4600e54007cb4707c9727b1171f56c17c80c16c53966535c57ab684e22
- 95c8ffe03547bcb0afd4d025fb14908f5230c6dc6fdd16686609681c7f40aca2
- 7c77ec259162872bf9ab18f6754e0e844157b31b32b4a746484f444b9f9a3836

Hacktool

MD5

- 3af4e21bbbeb846ca295143e03ec0054

SHA256

- efa57ca7aa5f42578ab83c9d510393fcf4e981a3eb422197973c65b7415863e7

Backdoor.Destover

MD5

- 7fe80cee04003fed91c02e3a372f4b01

SHA256

- 4fe3c853ab237005f7d62324535dd641e1e095d1615a416a9b39e042f136cf6b

---