RATANKBA: Delving into Large-scale Watering Holes

By Trend Micro (words)

Published: 2017-02-27 · Archived: 2026-04-05 21:44:02 UTC

In early February, several financial organizations reported malware infection on their workstations, apparently coming from legitimate websites. The attacks turned out to be part of a large-scale campaign to compromise trusted websites in order to infect the systems of targeted enterprises across various industries. The strategy is typically known as a "watering hole" attack.

It was all sparked by a spate of recent malware attacks on Polish banksnews article entailing a reportedly unknown malware in their own terminals and servers, along with the presence of dubious, encrypted programs/executables, and more prominently, suspicious network activity. More malware are delivered to the affected systems which were seen connecting to unusual and far-flung locations worldwide, possibly where company data are exfiltrated to.

The malware in question: RATANKBA. Not only was it tied to malware attacks against banks in Poland, but also in a string of similar incidents involving financial institutions in Mexico, Uruguay, the United Kingdom, and Chile. How did it infect their victims? Were there other malware involved? Does the campaign really have ties with a Russian cybercriminal group?

Based on the odd wording choices (in Russian) we saw used as commands within the malware, we construe that it is just a decoy—a tactic to obfuscate the attackers' trails. Banks weren't the only targets; among them are also enterprises in telecommunications, management consulting, information technology, insurance, aviation, and education. Also, the campaign wasn't just confined to North America and Europe, as we also observed a number of affected organizations in the APAC region, notably Taiwan, Hong Kong, and China.

Here we provide further analysis and insights that can complement other ongoing research into this threat.

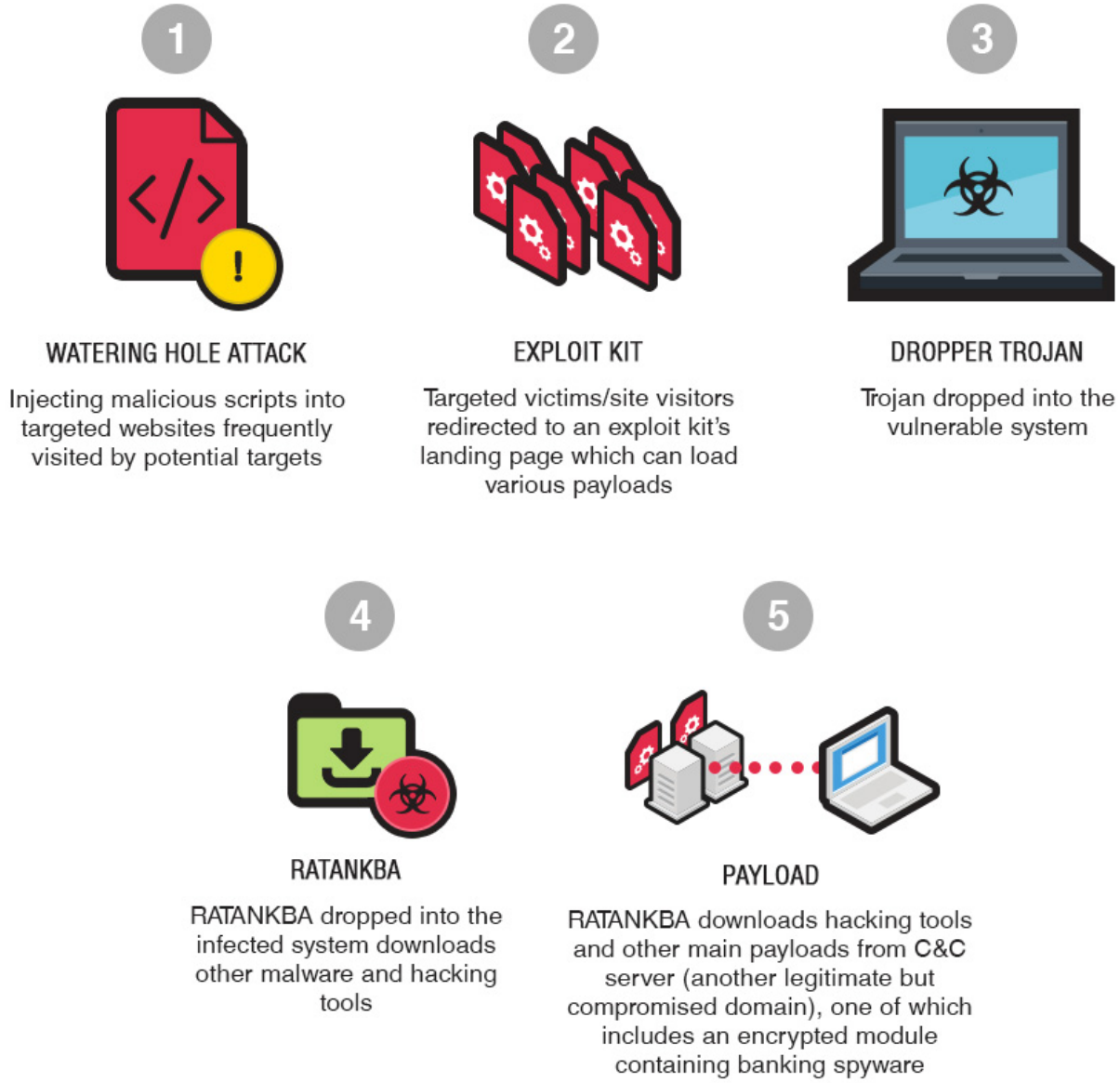

Figure 1. One of the possible infection flows involving RATANKBA

Infection Flow

The campaign, like what we saw in affected Polish banks, has many attack chains. The tools and techniques employed are typical in targeted attacks due to elements of lateral movement and reconnaissance. Malefactors used watering hole attacks to compromise legitimate and trusted websites frequently visited by their targets. These websites were injected with malicious JavaScript code that fingerprints browser components and loads vulnerability exploits from their malware and exploit kit-hosting systems, some of which were also likely compromised.

The infection is multistage and involves a variety of malware, with the final payload delivered only to their targets of interest. Different command and control (C&C) servers were used. Some were also compromised machines that

proxied connections to the attackers' infrastructure.

In one instance we observed, one of the initial malware delivered to the victim, RATANKBA (TROJ_RATANKBA.A), connects to a legitimate but compromised website (*eye-watch[.]in:443*, a mobile application-selling site) from which a hack tool (*nbt_scan.exe*) is also downloaded. The domain also serves as one of the campaign's platform for C&C communication.

The threat actor uses RATANKBA to survey the lay of the land as it looks into various aspects of the host machine where it has been initially downloaded—the machine that has been victim of the watering hole attack. Information such as the running tasks, domain, shares, user information, if the host has default internet connectivity, and so forth.

```
Process ID: 3424
Image Path: %windir%\system32\cmd.exe cmd.exe /c "netstat -ano | find "TCP" >> %TEMP%\TMPDC0C.tmp"

Process ID: 3408
Image Path: %windir%\system32\cmd.exe cmd.exe /c "tasklist /svc >> %TEMP%\TMPDC0C.tmp"

Process ID: 3392
Image Path: %windir%\system32\cmd.exe cmd.exe /c "reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings" >> %TEM
P%\TMPDC0C.tmp"

Process ID: 3376
Image Path: %windir%\system32\cmd.exe cmd.exe /c "net view /domain >> %TEMP%\TMPDC0C.tmp"

Process ID: 3348
Image Path: %windir%\system32\cmd.exe cmd.exe /c "net view >> %TEMP%\TMPDC0C.tmp"

Process ID: 3308
Image Path: %windir%\system32\cmd.exe cmd.exe /c "net user >> %TEMP%\TMPDC0C.tmp"

Process ID: 3268
Image Path: %windir%\system32\cmd.exe cmd.exe /c "query user >> %TEMP%\TMPDC0C.tmp"

Process ID: 3240
Image Path: %windir%\system32\cmd.exe cmd.exe /c "ping www.google.com >> %TEMP%\TMPDC0C.tmp"

Process ID: 3196
Image Path: %windir%\system32\cmd.exe cmd.exe /c "ipconfig -all >> %TEMP%\TMPDC0C.tmp"

Process ID: 3180
Image Path: %windir%\system32\cmd.exe cmd.exe /c "ver >> %TEMP%\TMPDC0C.tmp"

Process ID: 3152
Image Path: %windir%\system32\cmd.exe cmd.exe /c "whoami >> %TEMP%\TMPDC0C.tmp"
```

Figure 2. RATANKBA looking at different aspects of the machine

It would be worthwhile to note that RATANKBA has also been seen looking at specific IP ranges of interest:

```
Process ID: 2460
Image Path: %windir%\system32\cmd.exe /c netstat -a -n -o | findstr 198.

Process ID: 2376
Image Path: %windir%\system32\cmd.exe /c netstat -a -n -o | findstr 110.

Process ID: 2332
Image Path: %windir%\system32\cmd.exe /c netstat -a -n -o | findstr 103.

Process ID: 2288
Image Path: %windir%\system32\cmd.exe /c netstat -a -n -o | findstr 104.28.
```

Figure 3. RATANKBA looking for specific IP ranges

Our analysis of samples of the hack tool (HKTL_NBTSCAN.GA and HKTL_NBTSCAN.GB) indicate it as a command-line program that scans IP networks for NetBIOS information such as IP address, NetBIOS computer name, logged-in username, and MAC address—with some of the information coming from the initial RATAKNBA installation. The threat actor can now combine the information and brute force their way throughout the network (through NetBIOS) using a list of usernames and passwords as well as a range of IP addresses.

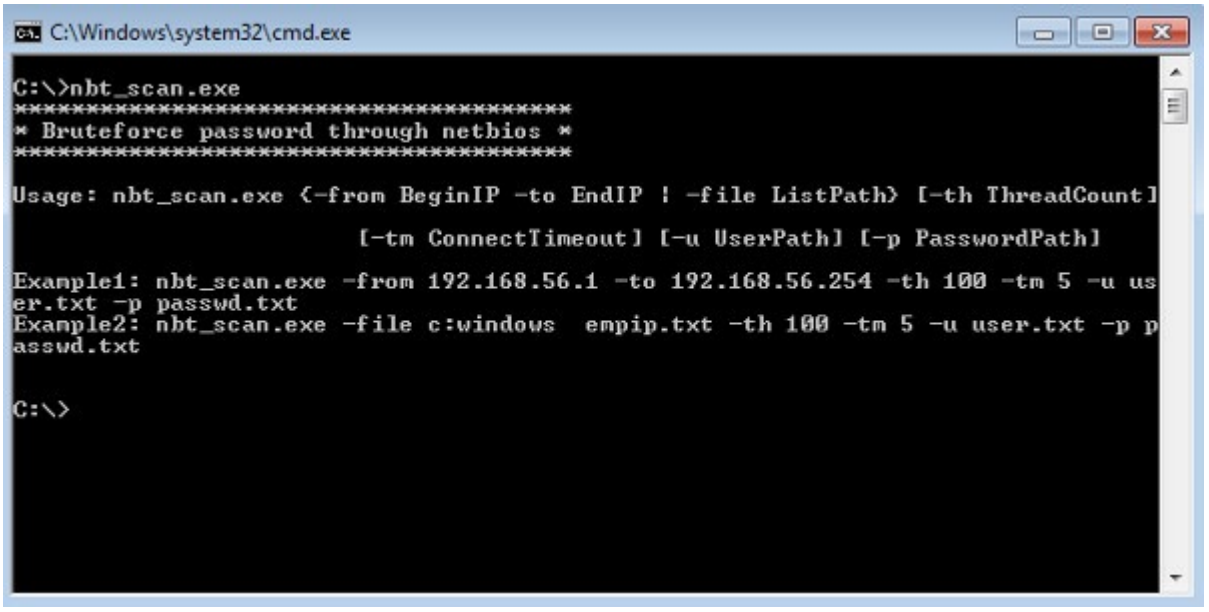

Figure 4. Commandline instructions of the hack tool

Upon successful connection, this hack tool will try to copy the *calc.exe* of the attacker's machine to the targeted computer's network share (C$) to test if file propagation via network share is successful and would most likely succeed if the credentials used would have administrative privileges. It then takes note of the infected machine's IP address, user, domain, hostname, OS and Service Pack, and the username and password combination that worked during the brute force routine. A log of it is then dumped to the directory where the file was initially executed.

With the combination of the information from RATANKBA and success/failure results from HKTL_NBTSCAN, the threat actor is now free to deploy final payloads to interesting hosts. A banking Trojan

(TSPY_BANKER.NTE) is among RATANKBA's final payloads. Some of the compromised sites used by attacker host several malware and suspicious/malicious files include:

An information-stealing backdoor (detected by Trend Micro as BKDR_DESTOVER.ADU),

A similarly named Flash file (*swf*, detected as SWF_EXPLOYT.YYRQ)

A Silverlight (.xap) file containing several files: an App Manifest (AppManifest.xaml), and DLLs Shell_siver.dll (TROJ_CVE20130074.B), and System.Xml.Linq.dll, which when repacked form a runtime remote code execution exploit for Silverlight (CVE-2016-0034, patched last January 12, 2016)

A Trojan (TROJ64_KLIPODLDR.ZHEB-A) that drops an encrypted module (BKDR64_KLIPODENC.ZHEB-A) containing a banking spyware (TSPY64_BANKER.YWNQD), used as a Windows service persistence mechanism DLL.

Impact

There were actually more victims than what was initially gauged. Feedback from our Smart Protection Network™ revealed that apart from attacks in North America (mainly the U.S.), Europe, and South America, the campaign also noticeably affected enterprises in Taiwan, Hong Kong, China, and Bahrain.

Affected organizations also included those in Luxembourg, France, the Philippines, Japan, Spain, Malaysia, Norway, and Romania. The targeted industries were consistent with other analyses: telecommunications (including internet service providers) and banking. We also saw a miscellany of targets whose industries comprise internet-related services (such as data center operations), management consulting, information technology, pharmaceutics, insurance, even aviation and education.

In the case of Taiwan, we've seen the compromised website diverting its visitors to another malware-hosting site that also acts as platform for C&C communication: *sap[.]misapor[.]ch*. We saw the affected websites of financial institutions in Uruguay and Mexico redirecting victims to the same URL. While the URL acts similarly to how *eye-watch[.]in:443* delivers payloads, we also saw the URL leveraging and exploiting security flaws in Flash: CVE-2015-8651, CVE-2016-1019, and CVE-2016-4117. These vulnerabilities were patched last December 28 2015, April 5, 2016, and May 12, 2016, respectively.

```
vaddr=0x0045e620 paddr=0x0005d220 ordinal=1046 sz=20 len=19 section=.rdata type=a string=kliyent2podklyuchit
vaddr=0x0045e634 paddr=0x0005d234 ordinal=1047 sz=7 len=6 section=.rdata type=a string=ssylka
vaddr=0x0045e63c paddr=0x0005d23c ordinal=1048 sz=13 len=12 section=.rdata type=a string=ustanavlivat
vaddr=0x0045e64c paddr=0x0005d24c ordinal=1049 sz=9 len=8 section=.rdata type=a string=poluchit
vaddr=0x0045e658 paddr=0x0005d258 ordinal=1050 sz=9 len=8 section=.rdata type=a string=pereslat
vaddr=0x0045e664 paddr=0x0005d264 ordinal=1051 sz=8 len=7 section=.rdata type=a string=derzhat
vaddr=0x0045e66c paddr=0x0005d26c ordinal=1052 sz=9 len=8 section=.rdata type=a string=vykhodit
vaddr=0x0045e678 paddr=0x0005d278 ordinal=1053 sz=8 len=7 section=.rdata type=a string=Nachalo
```

Figure 5. Screenshot of the malware's code showing commands in Russian

A False Flag?

The campaign notably bears similarities with activities that seem to point the finger to Russian perpetrators. Is there really a Russian connection? Delving into the malware, we found that it indeed uses commands in Russian—

transliterated from Cyrillic script to Latin alphabet, in particular. The verbs used were in their infinitive form, however, which is awkward for a command switch. Case in point: the use of “ustanavlivat” (“to install”) instead of the more command-like “ustanovit” (“do install”), which gives the impression that the malware operator lifted it from a dictionary or source where words are typically listed in default form.

Additionally, using verbs as commands is peculiar, especially for Russian cybercriminals or malware programmers who ironically eschew using Russian language in favor of broken English. Majority—if not all—of Russian programmers know that “connect” is keyed in as “connect”, because there’s already an API call (Application Program Interface) under that name. If you really have to use Russian, you’d rather use words like “vykhod” (“quit”) than “vikhodit” (“to exit”).

Another example is the use of “klyent2podklychit” we found within the sample we analyzed. The only intelligible part of it was “2”, which can be taken as “to” given how there’s an API call name for it (*client2connect*). In Russian, it’s practically gibberish, with the words wrongly ordered; it makes much more sense if “podkluchit_klienta” was used instead.

Indeed, with the awkward use of Russian language within the malware, we’re inclined to surmise it as more of a false flag, intentionally inserted in the code to flummox threat research and attribution attempts. It’s an uncommon tactic, but one that’s already been observed in other malware and cyberattacks.

Were the attacks carried out by cybercriminal group Lazarus? While there is ambivalence if they were indeed their handiwork, our analysis indicates that the malware codes and techniques employed resembled those used by Lazarus.

Mitigation

Security and system/IT administrators must practice due diligence in protecting their websites and web-based applications from threats that can undermine their security, and hijack them to do the bad guys’ bidding—delivering malware to their victims. Malicious web injectionsnews- cybercrime-and-digital-threats, for instance, leverage exploits that enable attackers to gain footholds into the system. An organization’s best defense is to regularly apply the latest patches, as well as routinely scan and examine traffic that goes through the enterprise’s network, which enables prompt incident response and remediation.

A multilayered approach is a must to securing the organization’s perimeter, especially for information security professionals and system/IT administrators. Hardening the endpoints is critical, as bad guys can use these to enter the company network. Implementing the apt restrictions/permissions policies on end user systems and employing application controlproducts can help prevent unwanted and suspicious applications and processes from being executed. Disabling unnecessary—or unused—components in the system such as third-party plugins and extensions helps reduce the system’s attack surface.

Employing firewalls and intrusion detection systems on top of proactive network monitoring can help mitigate incursions into the organization. This can be complemented by restricting direct internet access to the company’s internal networks while using proxies to access external resources. End users can help by practicing and fostering security habits, such as prudence against dubious and socially engineered links, emails, and websites.

Trend Micro Solutions

Trend Micro™ Deep Security™products and Vulnerability Protectionproducts provide virtual patchingproducts that protects endpoints from threats such as malicious redirections to malware-hosting URLs, as well as those that exploit unpatched vulnerabilities. OfficeScanproducts's Vulnerability Protection shields endpoints from identified and unknown vulnerability exploits even before patches are even deployed. Trend Micro™ Deep Discovery™products provides detection, in-depth analysis, and proactive response to attacks using exploits and other similar threats through specialized engines, custom sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect these attacks even without any engine or pattern update. Deep Discovery Inspector protects customers from these threats via this DDI Rule:

- DDI Rule 18 : DNS response of a queried malware Command and Control domain
- DDI Rule 15 : Many unsuccessful logon attempts (nbt_scan.exe)
- DDI Rule 38 : Multiple unsuccessful logon attempts (nbt_scan.exe)

TippingPoint customers are protected from these threats via these ThreatDV filters:

- 27218: HTTP: TROJ_RATANKBA_A Checkin
- 28219: HTTP: TROJ_RATANKBA_A Checkin 02
- 27220: HTTPS: TROJ_RATANKBA_A Checkin
- 27221: HTTP: Sundown EK Flash Exploit (SWF_EXPLOYT.YYRQ)

A list of related Indicators of Compromise (IoCs) can be found in this appendix.

Updated on February 27, 2017, 5:55 PM (UTC-7):
We updated the wording that cited affected organizations in several countries.

Updated on February 27, 2017, 11:08 PM (UTC-7):
We updated the section of the article that mentioned cybercriminal group Lazarus.

Updated on March 1, 2017, 09:15 PM (UTC-7):
An updated version of the appendix containing Indicators of Compromise (IoCs) and other technical details has been uploaded.
