

Meanwhile in Britain, Qadars v3 Hardens Evasion, Targets 18 UK Banks

securityintelligence.com/meanwhile-britain-qadars-v3-hardens-evasion-targets-18-uk-banks/

September 20, 2016



[Home](#) [Banking & Finance](#)

Meanwhile in Britain, Qadars v3 Hardens Evasion, Targets 18 UK Banks



[Banking & Finance](#) September 20, 2016

By [Limor Kessem](#) co-authored by [Hanan Natan](#) , [Denis Laskov](#) 7 min read

IBM X-Force Research reported that the operators of the [Qadars Trojan](#) have been progressively updating the malware's defenses and tailoring its configurations to target 18 banks in the U.K. In addition to its recent U.K. activity, the researchers found that Qadars campaigns launched in early September 2016 mainly targeted banks in the Netherlands, U.S. and Germany.

This activity comes on the heels of an uptick of [Ramnit Trojan attacks](#) against U.K. banks. After a period of relatively low activity, during which cybercriminals shifted their focus to Germany, Brazil and the U.S., it seems the U.K. is back on fraudsters' radar.

Qadars Makes the Rounds

From a global perspective, Qadars' operators have been making the rounds, targeting banks all over the world in separate bouts of online banking fraud attacks since 2013. By count of targeted brands, it appears the gang remains most inclined to attack in Europe.

Between 2013 and 2014, the malware mainly targeted banks in France and the Netherlands. Its top targets between 2015 and 2016 were Australia, Canada, the U.S. and the Netherlands. This past year, Qadars operators focused primarily on the Germany, Poland, the U.S. and the Netherlands.

[X-Force Research](#) indicated that while most of Qadars' targets have been banks, it is also after social networking credentials, online sports betting users, e-commerce platforms, payments and card services, among others.

Fueled by what appears to be experienced cybercrime factions, Qadars has been able to use advanced banking malware tactics ever since its early days, with capabilities such as:

Hooking the internet browser to monitor and manipulate user activity;

Fetching webinjections in real time from a remote server;

Supplementing fraud scenarios with an SMS hijacking app; and

Orchestrating the full scope of fraudulent data theft and transaction operation through an automated transfer system (ATS) panel.

ATS is fraudster lingo for a remote, web-based platform that Trojans access on the fly. The ATS panel contains transaction automation scripts, webinjections, preprogrammed transaction flow and parameters, transfer thresholds and mule account numbers on which the malware relies to complete illicit online transactions.

To steal two-factor authentication (2FA) codes from a user whose bank requires an out-of-band element, Qadars' operators deployed the [Perkele \(iBanking\) mobile bot](#) as the malicious mobile component. In this case, Qadars even added the theft of codes from mobile devices to the ATS transaction orchestration flow.

But Qadars didn't just use Perkele on bank transactions. It also targeted Facebook users who secured their accounts with 2FA, [HackRead](#) reported.

Qadars historically infects endpoints using exploit kits hosted on compromised hosts, or domains purchased for the purpose of serving malware. The Trojan was also pushed to user endpoints via botnets, leveraging downloader-type malware. In current campaigns, Qadars [leverages the Rig Exploit Kit](#) via the [EiTest campaign](#) to infect users, facilitating its infiltration with downloader malware.

[Read the white paper: Accelerating growth and digital adoption with seamless identity trust](#)

Qadars v3 Hits the Ground Running

Although Qadars emerged in 2013, it has not been widely documented compared to other advanced Trojans of its type. Under the hood, Qadars' developers borrowed code and fraud-facilitating concepts from the Zeus and Carberp Trojans, both of which had their source code leaked publicly in the past few years, thereby enabling malware authors to reuse parts of the code.

X-Force first detected Qadars v2 in October 2015. The present version, Qadars v3, was released in Q1 2016. Our researchers indicated that by May 2016, the malware's developer released detailed update notes for v3, all written in Russian, noting which bug fixes and improvements were made to the code, admin panel and ATS panel. The notes also provided information about browser and webinjection updates.

The release notes indicated that Qadars is an advanced online banking Trojan that comes from a single source. Its source programs all operational components and does not buy injection kits from outsourced developers. When Qadars v3 was detected in the wild, the malware's operators dedicated a new attack configuration to targeting all the major banks in Australia.

Qadars' fraud tactics are enabled through:

- Browser hooking (IE, Firefox);
- Cookie and certificate theft;
- Form grabbing;
- Webinjections;

- FIGrabbers and ATS;
- Use of the Tor client on the victim's machine to hide malware communications; and
- Use of domain generation algorithm (DGA) to hide remote malware resources (as of v3).

In terms of attack methods, Qadars is capable of in-session fraud, remote-controlling the infected endpoint via virtual network computing (VNC) and performing a fraudulent transaction in real time when the user is logged on. Qadars can also collect victim credentials and use them in account takeover fraud at a later time and from a different device, depending on the targeted bank and the corresponding authentication challenges.

Researching Qadars v3

Qadars v3 is continuously evolving. Yet another updated release in late August 2016 offered a new Qadars build with some code updates designed to evade detection, layer anti-research features, and improve the performance and readability of the malware's webinjection mechanisms.

The following section describes the technical changes made to the Qadars v3 in August 2016. This analysis was performed by malware researcher Hanan Natan and contributor Denis Laskov, senior security researcher at IBM Trusteer cybercrime labs.

Double Obfuscation on Dynamic API Resolution

Qadars' new version obfuscates all of its Win32 API calls by employing a common trick often used by banking malware of this grade, such as URLZone, Dridex and Neverquest. When the malware code starts to run and after the packer has completed its part, it dynamically resolves all the memory address of the APIs it's going to use.

Qadars contains hardcoded CRC32 values for all the function names it plans to use. This enables it to resolve the actual memory address of the function it will iterate over the export table of a particular system DLL and compare the CRC32 of the exported function name against the hardcoded one. If a match is found, Qadars saves the memory address of the function in a global variable.

The malware adds a twist to this well-known dynamic API resolving method by XORing the hardcoded CRC32 values of the function names with another constant value that's embedded in the binary itself. By employing this method, Qadars makes it a bit harder for scripts to find and annotate the actual Win32 APIs it uses.

In the following disassembly excerpt, we can see how the malware resolves the Win32 API addresses and saves them into global variables:



Internal Data Obfuscation

In the current Qadars version, we analyzed all the strings and data inside the binary that are XORed with a constant value that's embedded in the binary. Just before the malware uses a string or data, it first performs an inverse XOR operation on it.

Moreover, the malware added a compression layer for the configurations it downloads from the command-and-control (C&C) server. The compression layer was likely added due to the fact that webinjections, which are part of the configuration, have become larger and more sophisticated over time as more banks were added to the target list, making config files heavier and more easily detectable.

While previous versions of the malware downloaded configurations that were only encrypted using an AES algorithm, the new version adds compression after the encryption phase. The configuration ultimately gets decompressed on the infected endpoint using [aPLib](#), a [compression library](#) based on the algorithm used in aPACK.

Trojan Modules

Like other modular banking Trojans, such as [Shifu](#), for example, Qadars v3 downloads a number of extra modules from its C&C server to perform the actual malicious activities. The malicious payload, or the MainModule, as it was named by the malware developer, is responsible for fetching those additional modules from the C&C.

One of the MainModule's tasks is to inject the other downloaded modules into specific Windows processes according to the functionality of each module. It is possible to tell what task each module carries out according to a text string found in each one briefly describing its purpose:

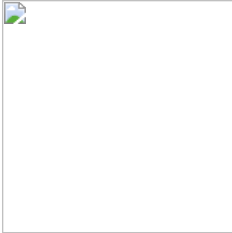
ModuleFailback_32.dll is injected into all processes and used as a watchdog to restart the malware in case of termination (persistence).

ModuleKeylogger_32.dll is injected into all processes to ensure data is keylogged properly.

ModuleBrowser_32.dll is injected into browser processes only. This module is used for downloading webinjections from the C&C and for managing the actual web fraud.

ModuleVNC_32.dll is injected into browser processes for launching remote control.

The names of the modules, as named by the developer of the malware, can be found in the DLL's export ordinal table. The moduleBrowser_32.dll even contains the path of the pdb file used during the actual development:



Additional changes in this version enrich the ability of the MainModule to download and use a Tor client to anonymize communications and covertly download modules from the C&C, ad hoc.

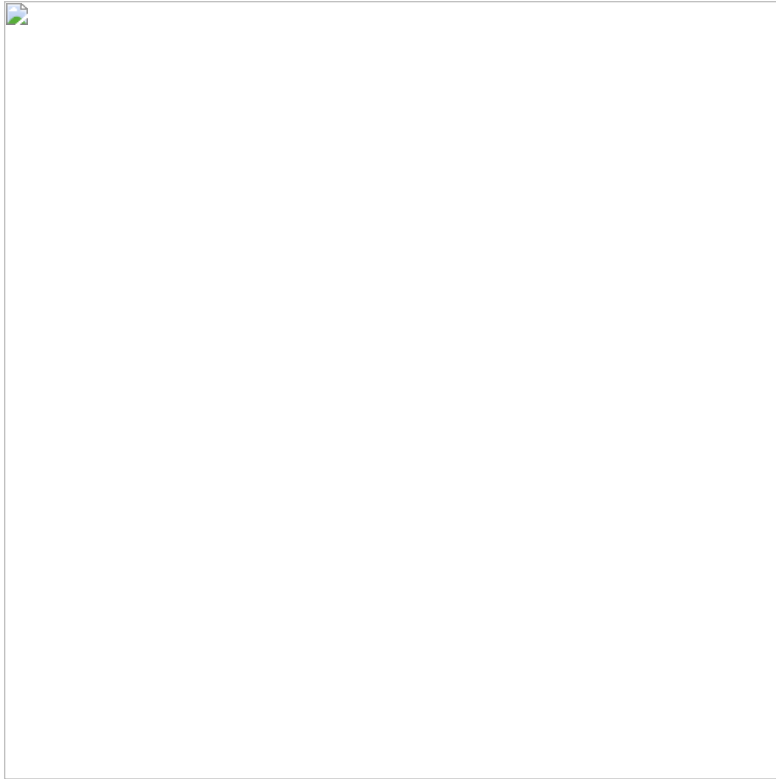
Privilege Escalation Tricks

To elevate its privileges on infected machines, Qadars' dropper can opt to display a social engineering message prompting the user to download a new Windows security update. That fake message is used to influence the user into unknowingly accepting a UAC prompt and inadvertently granting Qadars admin rights.



Once the user clicks the fake update notice window, the malware's dropper runs itself again using the ShellExecuteEx Win32 API. This time, however, the system displays a UAC dialog to the user.

The following figure shows an excerpt of the decompiled code. The malware doesn't give the user an option to cancel or close the fake update window. Basically, users will encounter the UAC prompt again and again until they approve it, at which point the malware is launched again, this time with a new, higher privilege level:



Conclusion

Qadars attack volumes, compared to Trojans like Neverquest or Dridex, are more humble. While it is not one of the top 10 financial malware threats on the global list, however, this Trojan has been flying under the radar for over three years, attacking banks in different regions using advanced features and capabilities. It's possible that Qadars attack volumes remain limited because its operators choose to focus on specific countries in each of their infection sprees, likely to keep their operation focused and less visible.

On the technical side, Qadars is an active and evolving malware project, as are other malicious codes of its type. In that sense, this threat is as advanced and problematic as other banking Trojans, such as [Gozi](#), [Tinba](#) or Ramnit. The language used in the Qadars v3 release notes suggests the malware developer is most likely a Russian-speaking black hat.

Qadars' operators are well-versed in orchestrating the malware infection operation by leveraging exploit kits, launching fraudulent transactions from infected endpoints and circumventing 2FA by infecting victims' mobile devices.

Beyond the preprogrammed parts of its configuration files, Qadars relies on communication with remote servers and ATS panels to fetch money mule account numbers in real time. It also displays social engineering injections delivered from its servers in real time and can enable hidden remote control of infected machines to defraud their owners' accounts.

Malware IOCs

Dropper MD5

Some MD5 hashes are:

- [1979D1E5E9395025BC395BA00DF824CA](#)
- 236034B533B76A025AE353F3577DC298
- 26E2ECBDAEF376376141D5B42998D4CA
- 394BED68BB412F26F8DF71874D346B9B
- 63246F89F57498EDE2796169EA597DEF

AV Detection Aliases

Presently, Qadars may not be detected as such by all anti-virus software. Current aliases from top AV vendors detect the dropper's executable sample as:

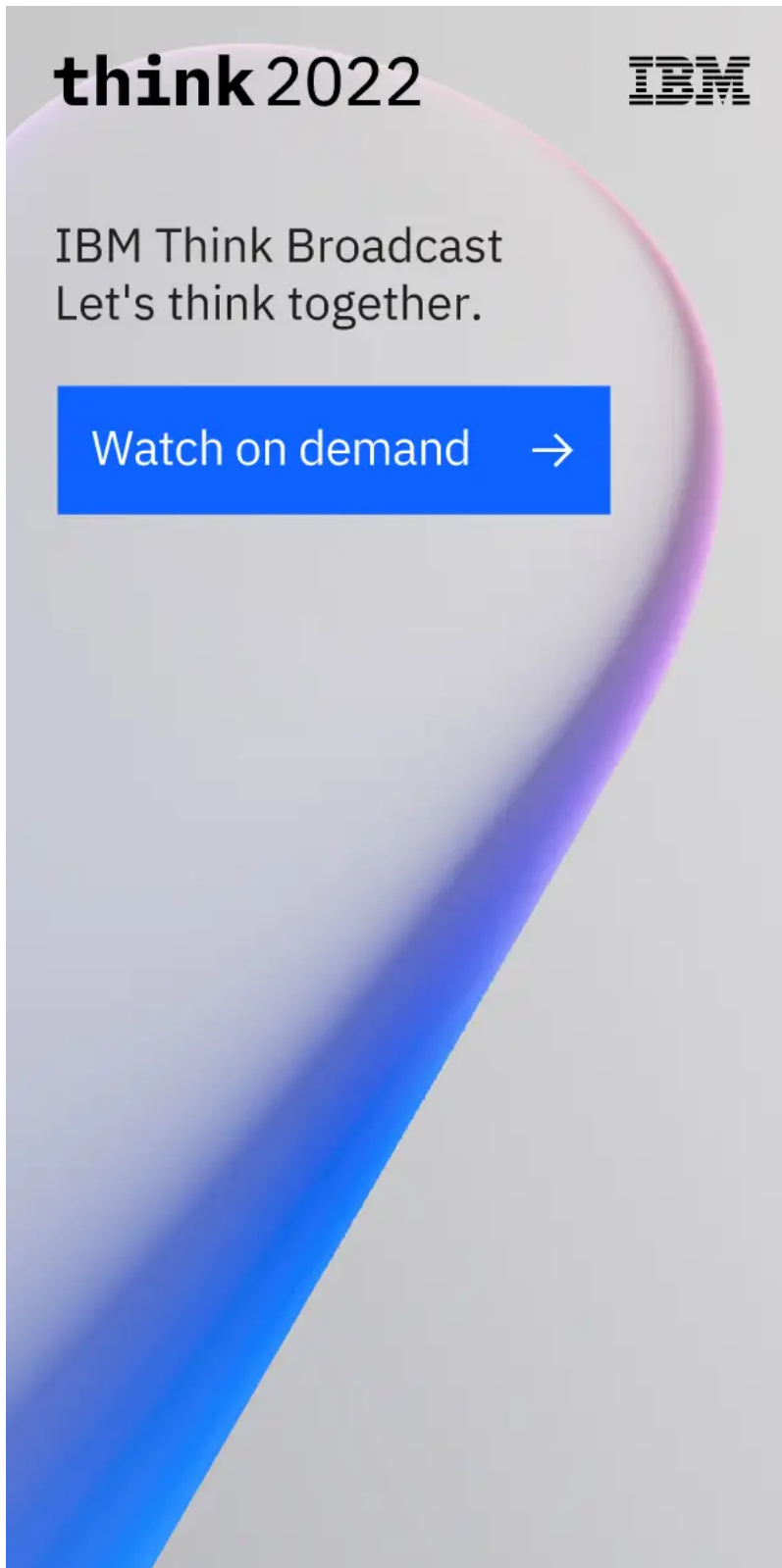
- Win32/Sopinar.G
- Trojan.Win32.Yakes.qpxg
- BehavesLike.Win32.PWSZbot.dh

- Heur.AdvML.B

Limor Kessem

Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...

The image is a promotional graphic for the IBM Think 2022 Broadcast. It features a light gray background with a large, curved, abstract shape on the right side that transitions from light purple at the top to bright blue at the bottom. In the top left corner, the text "think 2022" is written in a bold, lowercase sans-serif font. To its right is the IBM logo in its classic striped font. Below the "think 2022" text, the words "IBM Think Broadcast" are written in a clean, sans-serif font, followed by the tagline "Let's think together." in a slightly smaller font. At the bottom of the text area, there is a blue rectangular button with the white text "Watch on demand" and a white right-pointing arrow.