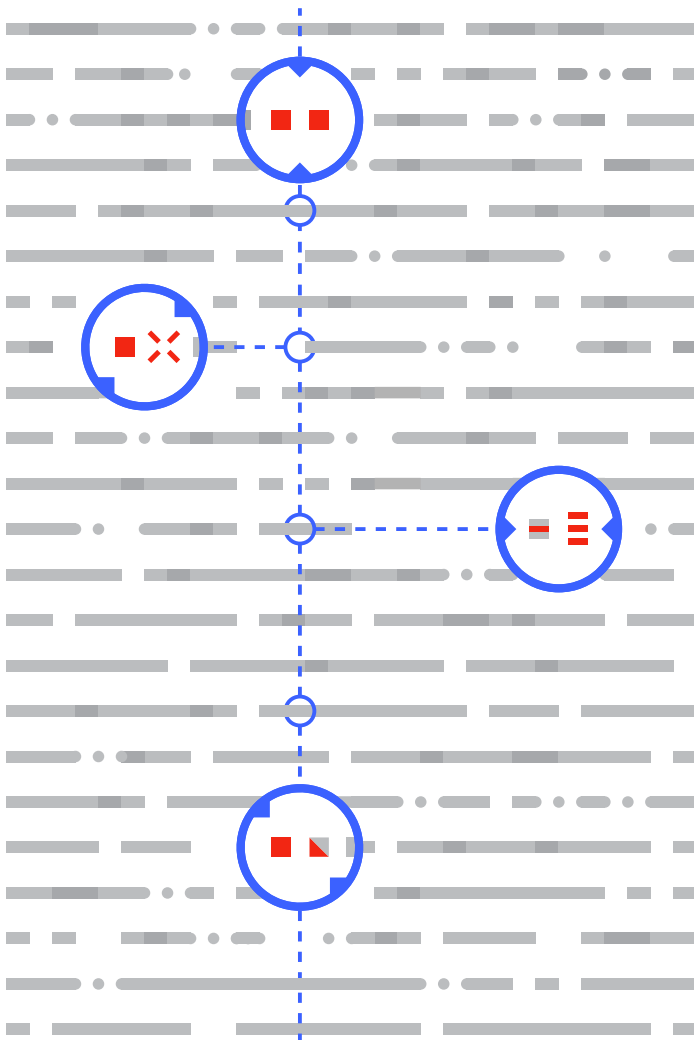


# VTI for Banking Trojans

## Using VirusTotal Intelligence to disable banking trojans

For financial services firms, banking trojans can cause financial and reputational harm. VTI provides intelligence that can reduce the effects of this industry-targeted malware.



**Problem:** Financial services firms, especially retail banks, are major targets for fraud. Threats include phishing, trojans, and other types of malware. Taken as a group, these threats impact both the reputations and operating costs for financial firms.

**Solution:** While these threats cause significant pain, they can also be significantly reduced, with the right techniques. VirusTotal Intelligence provides advanced functionality for preventing or reducing targeted banking attacks.

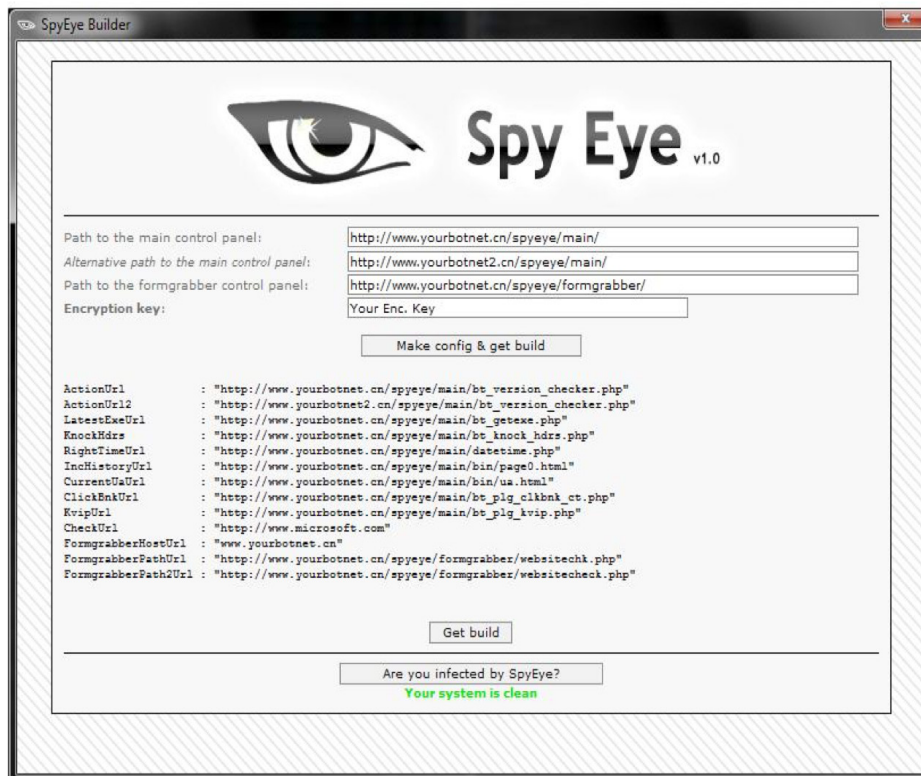
**Use Case:** Use VirusTotal to discover banking trojan families, write rules to receive notifications upon analysis of new variants of tracked families, download samples and apply plugins to automatically reveal malicious network infrastructure. This paper describes five steps for shutting down banking trojan attacks, and a bonus step for handling customer phishing attacks.

As banking transactions and commerce have moved online, so has fraud and theft. Hacking for fun has shifted to hacking for profit (interception of banking credentials, credit card details theft, online identity impersonation, machine rescue ransoms, etc.) and phishing campaigns and banking trojans have become pervasive on the Internet. In many countries, these attacks are not only a problem for the victims but also for the banks and financial institutions that may be liable and forced to refund

the stolen amounts. Even when this is not the case, customer trust and brand reputation are at stake.

The term *banking trojan* is used to designate a piece of malware that targets funds from an online bank account. Certain other financial services such as online stock brokerage services, online payment systems, pension plan portals, etc. are also common targets. Strong passwords, SSL certificates, secret tokens and two factor authentication are not enough against these threats as they live in your customers' systems and will inject fraudulent code into banking web pages as they are loaded into customers' browsers. Trojans can entice users to download further malicious applications onto their phones, visually faking their account's balance, etc.

Banking trojan authors often create builder kits that allow non-technical attackers to customize and build new variants of a given trojan, leading to hundreds of malware instances produced by a *tool for dummies*.



Similarly, attackers will often use server and client-side polymorphism to generate hundreds of distinct binaries for the same campaign in order to make analysis more complex. This is how thousands of binary-distinct threats end up in VirusTotal from all over the world.

Leverage the power of [VirusTotal Intelligence](#) search capabilities and [YARA](#) malware hunting to:

- Gain insight into phishing and malware attacks that may target your organization
- Discover emerging threats and the latest technical and deceptive attack techniques
- Spot fraud in-the-wild, identify network infrastructure used to steal credentials, and take measures to mitigate ongoing attacks
- Track the evolution of known bad actors that have targeted your organization in the past and stay ahead of them

This paper will show you how.

---

[CONTACT US](#) for more information on service offerings and pricing:

[info@virustotal.com](mailto:info@virustotal.com) / [www.virustotal.com](http://www.virustotal.com)

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED

## Step One: Discover New Threats

Think of VirusTotal Intelligence as the “Google of malware,” allowing you to search for samples using a combination of over 40 search modifiers to filter a dataset of nearly 2 billion files, growing at a rate of over 1 million new files a day. Malware analysts can use VTI to discover new banking trojans and infostealers by regularly searching for interesting malware flying under an organization’s radar. For example:

engines:banker OR engines:banking OR engines:infostealer

*Return all those samples that have been detected by at least one antivirus solution with a label containing the word banker, banking or infostealer.*

tag:suspicious-dns AND engines:banker

*Files that make use of a domain generation algorithm (stealthy command and control and theft drop zone infrastructure) and detected by at least one antivirus solution as a banker.*

You can also use the search engine to access the latest threats referenced in private fraud mailing lists, work groups and common industry information sharing forums, blog articles, etc.



The screenshot shows the VirusTotal Intelligence search interface. The search bar contains the query 'engines:banker OR engines:banking OR engines:infostealer'. Below the search bar, it indicates '1000+ files found'. A table displays the search results with the following columns: File, Ratio, First sub., Last sub., Times sub., Sources, and Size. The first result is a file with a long hash, a ratio of 35 / 68, first submission on 2017-10-21, last submission on 2018-02-11, 92 times submitted, 1 source, and a size of 127.0 KB.

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
d75f7d020b571f10dd17326a456efbc767ecd8c6b20c72cc173646bf805470df	35 / 68	2017-10-21	2018-02-11	92	1	127.0 KB

Once you have identified interesting study candidates, VirusTotal Intelligence allows you to download the pertinent samples for further inspection and reverse engineering.

Next, use your favourite debugger and disassembler to uncover the web injection mechanism used by the trojan to deceive your users, thus identifying how the stolen data is communicated back to the attacker and how the piece of malware narrows its focus to intercept credentials from your customers.

## Step Two: Reveal Similar Files

In order to build a robust rule against a given malware strain, understand its context fully and uncover tactics, techniques and procedures used by the attackers behind a given threat, you need to identify other specimens pertaining to the very same malware family.

VirusTotal has developed an in-house feature hash that clusters samples together and allows you to search for files sharing similar characteristics making use of the similar-to search modifier. Other de facto industry standards such as imphash or ssdeep can also be used to identify other files belonging to the same family that you have just uncovered.

---

**CONTACT US** for more information on service offerings and pricing:

info@virustotal.com / www.virustotal.com

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED

similar-to:87dbf7b18a807f423e1681e6f049003a3bb3b24e65bff625d4e316791e1f3735 Search Hashes Select Download

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
<input type="checkbox"/> 87dbf7b18a807f423e1681e6f049003a3bb3b24e65bff625d4e316791e1f3735 367f7ca8f3514513d11e5755cb6f4b9d peexe assembly	16 / 68	2018-02-11 16:39:24	2018-02-11 16:39:24	1	1	738.5 KB
<input type="checkbox"/> f5ab4471cde4adec2d6b8b00f22cd3fe35c735e888fa212ebdf8d24c38cdce8 610a0e3ea2c86360706042c4ffebaf30 peexe assembly	22 / 59	2017-03-12 22:29:43	2017-03-12 22:29:43	1	1	684.0 KB
<input type="checkbox"/> 0c5c62b61e808ff43f5500681da9c72efb64633f4d151c0bdfcc95e819811aee da170619b39f871d8dfd1fc395cb4263 peexe assembly	37 / 55	2015-12-31 16:18:57	2015-12-31 16:18:57	1	1	780.0 KB
<input type="checkbox"/> 7fc3a42c66bb30d95269bff1e5c40d259bd9264d503888a577b5e55ebef69500 f14f3ed27d89d476d2c6710af8a978ba peexe assembly	17 / 56	2015-12-01 09:07:36	2015-12-01 09:07:36	1	1	712.0 KB

Searching is not only limited to binary or structural similarity. All of the metadata attributes that you see on VirusTotal reports may be leveraged to find other samples that share commonalities, these may range from a fake product name used in the FileVersionInfo properties to portable executable section names.

Now that you have a collection of samples all belonging to the new malware family that you have **uncovered**, you may use VirusTotal Intelligence's batch download functionality in order to study the samples locally and extract common binary patterns from the matching samples. **Use these patterns** to build rules that will allow you to identify future campaigns making use of the same family and track its evolution.

### Try it Yourself

*Files similar to a password stealer.*

[similar-to:1586ee2d8fcd384ed5193a5d184980e1e223b59ba9c4641d87d3f47f3e400893](#)

*Banking trojans are often produced with kits for dummies, meaning that they often share the very same server-side setup to collect stolen data and act as a command and control center. Server-side paths are often shared among distinct campaigns using a same family.*

[behaviour: "/panel/gate.php"](#)

*CARBERP is an online banking Trojan that was first seen in 2009. It is designed to steal user credentials through hooking network APIs in WININET.DLL. All variants of a particular campaign using CARBERP shared a common set of FileVersionInfo properties.*

[sigcheck:Hysterically AND sigcheck:synapticula](#)

## Step Three: Write Evolution Tracking Rules

VirusTotal has developed [YARA](#), a pattern-matching Swiss Army knife for malware researchers. With YARA, you can create

**CONTACT US** for more information on service offerings and pricing:

info@virustotal.com / www.virustotal.com

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED

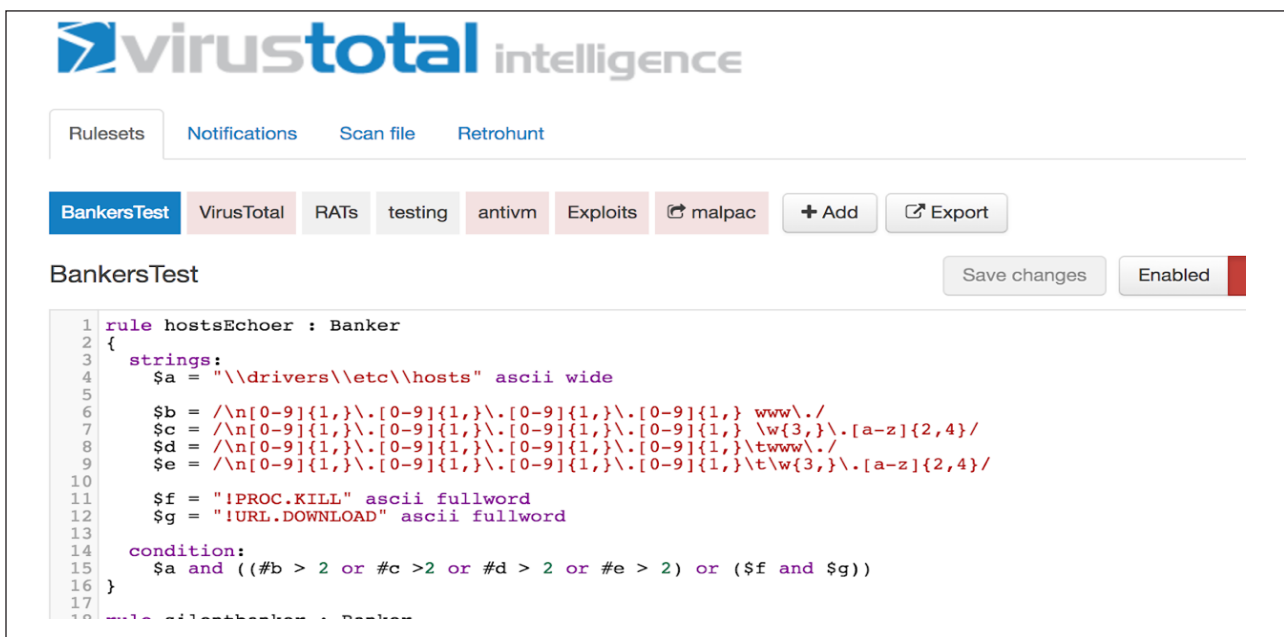
descriptions of malware families (or whatever you want to describe) based on text or binary patterns. Each description, also known as rule, consists of a set of strings and a boolean expression which determine its logic. For example:

```
rule Delephant : Banker
{
  meta:
    description = "Delphi banking trojan targeting brazilian banks via browser window overlays."

  strings:
    $a = /Conta[\.]{3,}/
    $b = /Nome[\.]{3,}/
    $c = "Tabela de Senhas" ascii

  condition:
    $a and ($b or $c)
}
```

VirusTotal Intelligence includes capabilities for malware hunting that enable you to write and store rules that will be matched against all future file submissions, over 1 million files daily.



The screenshot shows the VirusTotal Intelligence web interface. At the top, there's a navigation bar with 'Rulesets', 'Notifications', 'Scan file', and 'Retrohunt'. Below that, there's a row of buttons for different rule categories: 'BankersTest', 'VirusTotal', 'RATs', 'testing', 'antivm', 'Exploits', 'malpac', '+ Add', and 'Export'. The 'BankersTest' rule is selected and shown in a code editor. The rule is named 'hostsEchoer' and is of type 'Banker'. It contains several strings and a condition. The strings are: '\$a = "\\drivers\\etc\\hosts" ascii wide', '\$b = /\n[0-9]{1,}\. [0-9]{1,}\. [0-9]{1,}\. [0-9]{1,} www\./', '\$c = /\n[0-9]{1,}\. [0-9]{1,}\. [0-9]{1,}\. [0-9]{1,} \w{3,}\. [a-z]{2,4}/', '\$d = /\n[0-9]{1,}\. [0-9]{1,}\. [0-9]{1,}\. [0-9]{1,}\twww\./', '\$e = /\n[0-9]{1,}\. [0-9]{1,}\. [0-9]{1,}\. [0-9]{1,}\t\w{3,}\. [a-z]{2,4}/', '\$f = "!PROC.KILL" ascii fullword', and '\$g = "!URL.DOWNLOAD" ascii fullword'. The condition is '\$a and ((#b > 2 or #c > 2 or #d > 2 or #e > 2) or (\$f and \$g))'. There are 'Save changes' and 'Enabled' buttons to the right of the code editor.

To ensure that your rules have good coverage and low false positive rates, and to identify the first variants of the target malware family, you may run a retrohunt, which executes your rule retroactively against the existing collection of files in VirusTotal. When a new file matching your rule appears in VirusTotal, you will be notified, via the web platform, email or programmatically through an API.

[CONTACT US](#) for more information on service offerings and pricing:

[info@virustotal.com](mailto:info@virustotal.com) / [www.virustotal.com](http://www.virustotal.com)

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED

File	Date	Ruleset	Matching rule
e6dd6078cacae25c2b333c2a85cd17d8ad2528b459be3435d195e92f681c09d8 97bb219a...	2018-02-10	bankers	SilentBanker
c4326ce2... a8a14bd4...	2018-02-10	bankers	Dyre
63cdeb0... 4eb46c24...	2018-02-10	bankers	Trickbot
775febeffe... 8f39d98ae...	2018-02-10	bankers	ProxyAutomationConfig
b19cf8347... 2984c564...	2018-02-10	RATS	Bozok
3f12f6c55cec6bcd11ae6d3ab05fd1b9f3e4332a209a8375535e15ab6d05d0a7	2018-02-04	RATS	Bozok

It is crucial to track new variants of pertinent malware families, as this enables you to:

- Connect the dots and complete the attribution picture
- Understand new deception techniques used to disseminate the trojan
- Reveal morphing functionality and identify new mechanisms to attack your customers and harvest their data
- Identify network infrastructure being used by new attacks -- this is important, as you can shut it down to prevent collection of stolen data and remote control of infected machines

### Step Four: Prevent Data Theft and Mitigate Fraud

Since banking customers use their own devices to access their online accounts, you likely do not have visibility into these infected devices, nor the ability to control them. However, by identifying the malicious network infrastructure being used by attackers, your team can contact the pertinent hosting companies and registrars to shutdown the data collection servers and prevent theft.

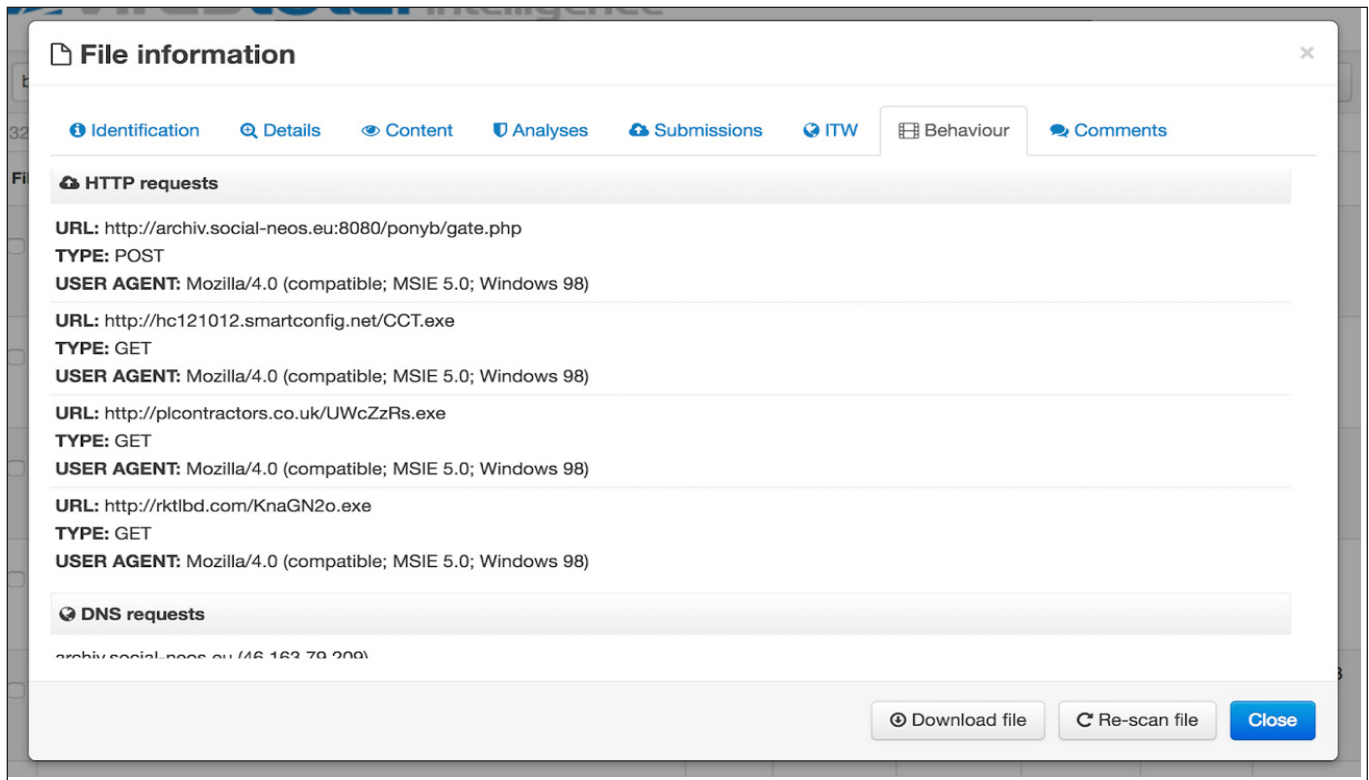
Moreover, many banking trojan families will download a configuration file from a web server that will contain the set of banks and financial institutions to target, along with the pertinent man-in-the-browser functionality to implement upon visiting each of the attacked banking sites. By shutting down the configuration file dissemination point, further fraud can be stopped.

VirusTotal will **execute incoming files in a virtual environment, to trace their network communications and system actions.** VirusTotal Intelligence displays the resulting reports for each sample and can often reveal the relevant fraud network infrastructure.

**CONTACT US** for more information on service offerings and pricing:

info@virustotal.com / www.virustotal.com

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED



Even when this is not the case, and further work is required to uncover malicious network infrastructure, you may leverage VirusTotal's Private API to automate the download of every YARA notification. You can then run them in your own sandboxing systems with family-specific plugins that will decipher configuration files, extract network infrastructure from memory dumps, etc.

You now have a threat research lab setup that automatically narrows down VirusTotal submissions to malware families of interest to you and extracts artifacts to allow your team to shutdown malicious infrastructure and prevent fraud.

Deeper manual inspection of your YARA notifications may also allow you to identify the HTML sequences the trojan is scanning in your company's web apps, to perform its man-in-the-browser injections, which URL patterns is it looking for in order to target specifically your customers, etc. **This information can be leveraged to make small tweaks to your site and render all variants of the same attack ineffective.** For instance, if a trojan is looking for the URL pattern `*/wcmfd/wcmpw/CustomerLogin*`, by simply modifying your path structure to `/new/CustomerLogin` you will immediately stop the effectiveness of the attack.

## Step Five: Gain Context, Know Your Enemy, and Stay Ahead

For every threat you research, VirusTotal Intelligence presents a profile page that contains far more detail than is available in the public reports:

- **Submission metadata** can be used to understand the attacks timeline and prevalence: When was a file first seen in-the-wild? Where are most of its victims located? Do the submission filenames reveal social engineering tricks used by attackers?

---

**CONTACT US** for more information on service offerings and pricing:

[info@virustotal.com](mailto:info@virustotal.com) / [www.virustotal.com](http://www.virustotal.com)

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED

#### Download URLs

This file has been spotted as the response content of the following URLs.

<http://flashpointy.xyz/panel2/module2.exe>

- **Relationship details** can be used to connect your artifacts with other files in the collection and to uncover new tools used by attackers. These collections of files bring even more context to your investigation. Similarly, **in-the-wild** information allows you to pinpoint and shut down URLs being used to deliver the trojans, and to discover emails used to propagate the threat, giving you insight into the language and deceptive tricks attackers are using to fool your customers into executing their malware files.

[Identification](#) [Details](#) [Content](#) [Analyses](#) [Submissions](#) [ITW](#) [Comments](#)

---

#### Prevalence metrics

<b>First submission</b>	2014-07-02 15:30:46
<b>Last submission</b>	2018-02-11 14:18:00
<b>Number of submissions</b>	67
<b>Distinct source submissions</b>	35

---

#### Propagation, dissemination and distribution strategies

This file has been spotted in-the-wild travelling as email attachments, some of these emails are later on detailed.

---

#### Attached in emails

- [+] Scanned from a Xerox Multifunction Device ("Accounting@showtimechoo.com" <Accounting@showtimechoo.com>)
- [+] Scanned from a Xerox Multifunction Device ("Accounting@sannoroo.com" <Accounting@sannoroo.com>)
- [+] Scanned from a Xerox Multifunction Device ("Accounting@dolidoli.com" <Accounting@dolidoli.com>)
- [+] Scanned from a Xerox Multifunction Device ("Accounting@rmgcal.com" <Accounting@rmgcal.com>)

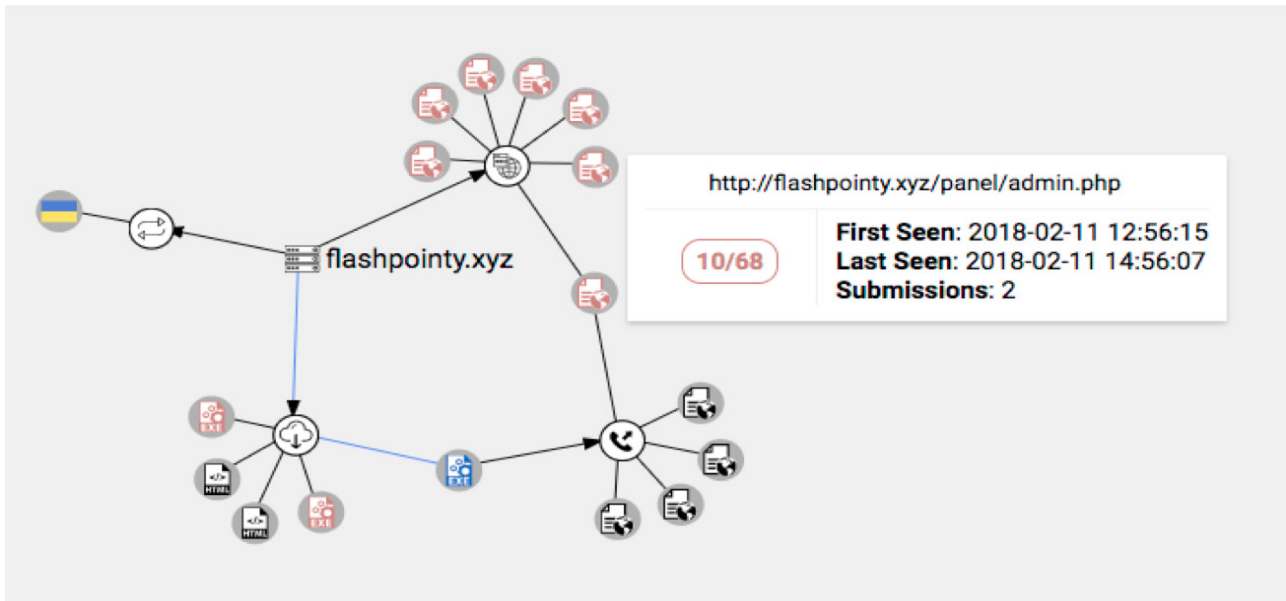
For each studied sample you may also pivot according to their contacted domains, created mutexes, downloaded URLs, etc. in order to uncover other connected malware that may give you further insight into the actors behind the attack. Connect the dots using VirusTotal Graph and discover visually malicious behaviors that may have gone unnoticed.

[CONTACT US](#) for more information on service offerings and pricing:

[info@virustotal.com](mailto:info@virustotal.com) / [www.virustotal.com](http://www.virustotal.com)

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED





## Bonus Track: Uncover Customer Phishing Attacks

Banking trojans are one of the most troubling threats your customers may face. Trojans live in customers' computers and phones, and can alter your legitimate site to ask for and intercept all data points needed to perform unauthorized funds transfers. However, humans are the weakest point of your security strategy, and so less advanced attacks often will be enough to steal from your clients and damage your reputation. As such, phishing should not be neglected. It is used in conjunction with social engineering techniques to gain access to all secrets needed to perpetrate theft.

You may know that the [VirusTotal's Private API](#) allows you to retrieve information about files, URLs, domains and IP addresses. The API also gives you access to a set of feeds. The URL feed contains all URLs scanned by VirusTotal. By syncing up with the URLs received, you may run typosquatting algorithms on the URLs and inspect the server-side responses to uncover sites that may be trying to impersonate your brand.

Interested in learning more or seeing a custom, live demo? Drop us a line at [info@virustotal.com](mailto:info@virustotal.com).

---

**CONTACT US** for more information on service offerings and pricing:

[info@virustotal.com](mailto:info@virustotal.com) / [www.virustotal.com](http://www.virustotal.com)

(C) 2018 VIRUSTOTAL ALL RIGHTS RESERVED