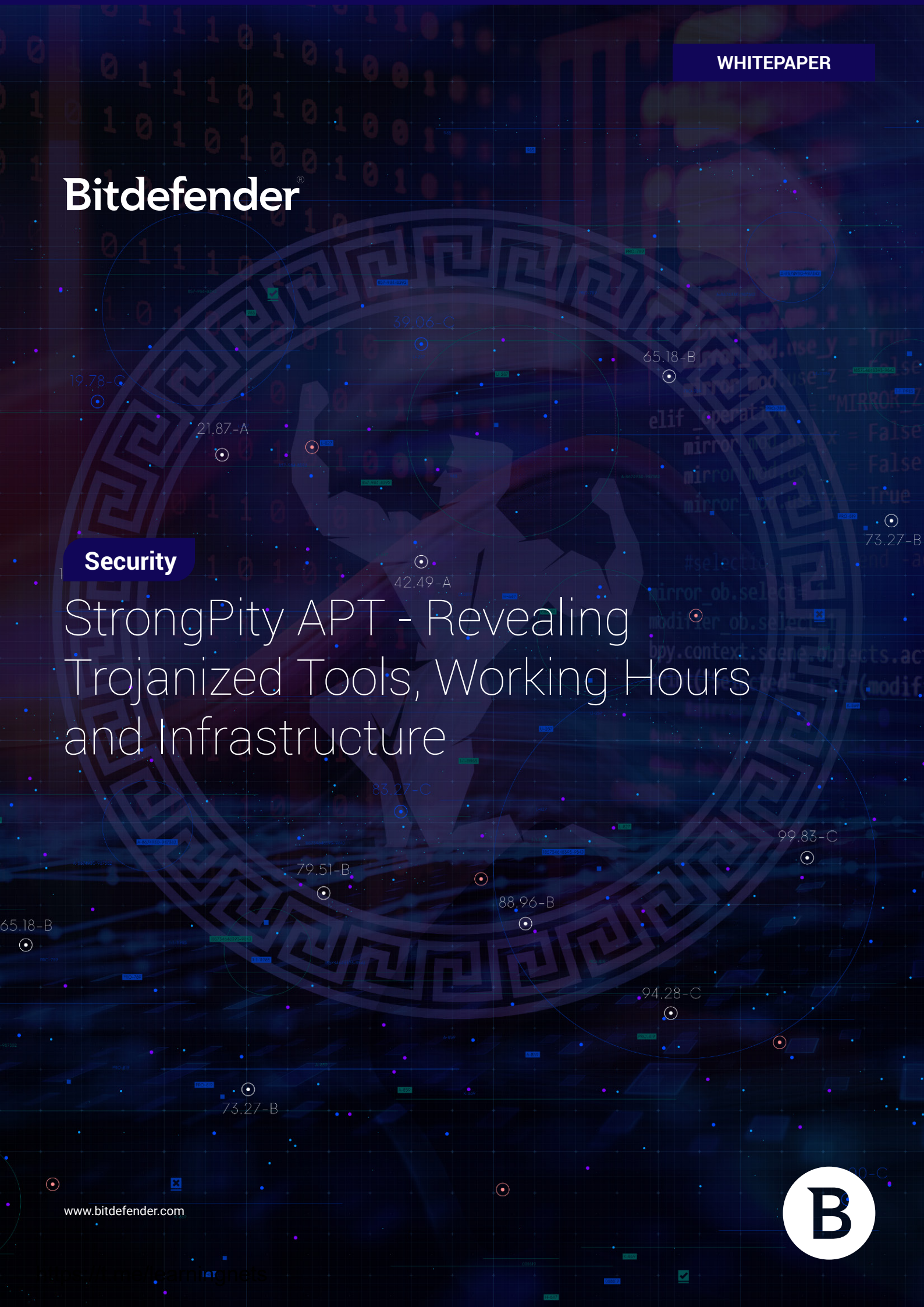
WHITEPAPER

Bitdefender

Security

StrongPity APT - Revealing Trojanized Tools, Working Hours and Infrastructure



www.bitdefender.com

Contents

Author:

Radu Tudorica – Security Researcher, Cyber Threat Intelligence Lab

Co-authors:

Cristina Vatamanu - Senior Team Lead, Cyber Threat Intelligence Lab

Alexandru Maximciuc - Team Lead, Cyber Threat Intelligence Lab

Overview

StrongPity, also known as Promethium, is a threat group that is assumed to have been active since at least 2012. Information about this actor was first publicly reported in October 2016 with details on attacks against users in Belgium and Italy. Later, in 2018, the attackers shifted their focus on another geographical region, compromising Turkish telecommunication companies to target hundreds of users in Turkey and Syria.

It is believed that the attacks attributed to StrongPity are government-sponsored and are used for population surveillance and intelligence exfiltration. More so, it is believed that these attacks are used as support for the geo-political conflicts in the region.
The known preferred infection vector used by the StrongPity group is a watering hole technique, delivering malicious versions of legitimate installers to certain targets.

By closely monitoring this threat, Bitdefender has managed to investigate it from several angles. Besides the technical setups of command and control servers, our researchers managed to get an insight into the victims' profile.

Most of the targets are located in two regions in Turkey: in Istanbul and the area close to the Syrian border.

The data we have gathered in the investigation into this threat actor suggests that the attacker is interested especially in the Kurdish community, placing this threat in the geo-political context of the constant conflicts between Turkey and the Kurdish community.

Key Findings:

- Watering hole tactic that selectively targets victims in Turkey and Syria using pre-defined IP list
- 3-tiered C&C infrastructure for covering tracks and thwarting forensic investigation
- Use of fully-working Trojanized popular tools, compiled during working hours

Infrastructure

During the time we closely monitored this threat actor and investigated different points from their infrastructure, we were able to distinguish two types of servers, used to fulfill two main roles:

- Servers that will serve the poisoned installer used in the initial compromise (referred from this point on as Download Servers)
- Servers used for exfiltrating information and for interacting with the victim through commands (referred from this point on as Command and Control Servers)

Some particularities for each of these types will be detailed below.

Download Servers

As mentioned before, one of the preferred infection mechanisms is a watering hole technique. In this type of attack, the threat actor will make use of certain websites that the victim often visits. For what was observed in the wild, StrongPity actors were able to tamper some localized software aggregates and sharers.

Usually, website visitors, when trying to download a certain installer, are redirected to a dedicated download server, as a result of a rewritten request to the legitimate server. If a user is of interest to the threat actor (his/her IP address is within one of the ranges it targets), the server will return the tampered version of that installer. Otherwise, the user will receive the original version of it.

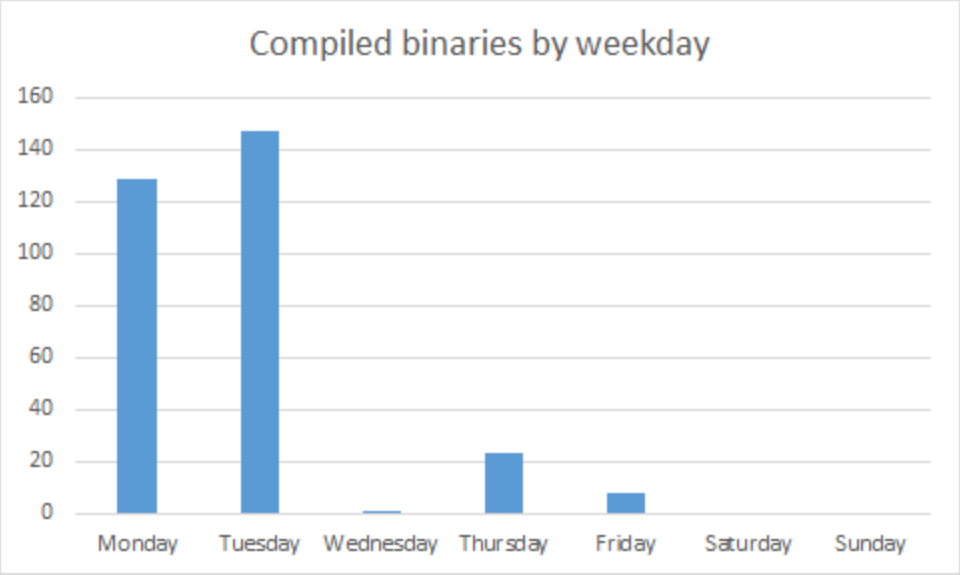
The servers where the targeted users are redirected are referred as the ***download servers***.

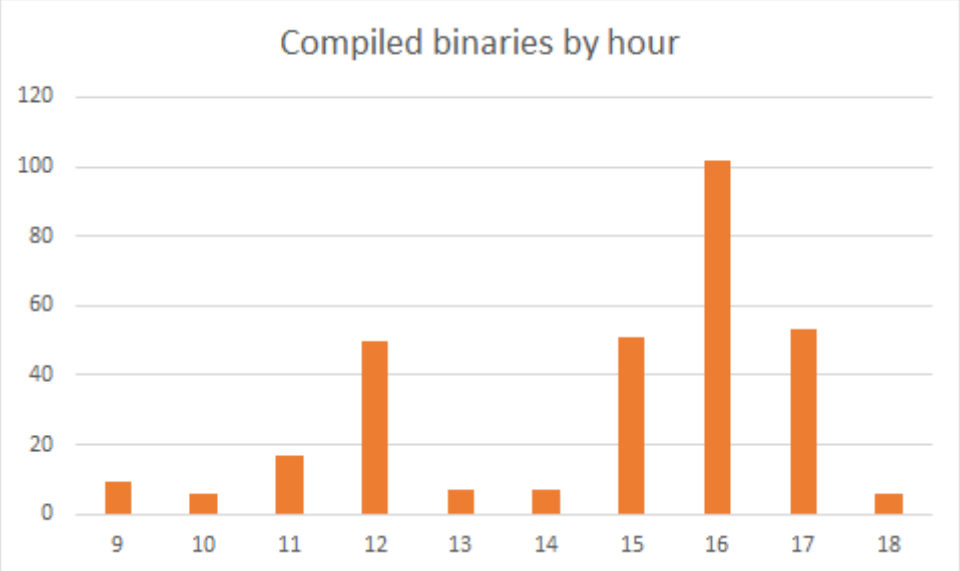
Trojanized installers

The malicious installers, which are served to the targeted victims, are quite interesting. The actor uses a custom bundler/dropper, digitally signed (with a self-signed certificate), that embodies the malicious components and the original, legit software product. But these initial droppers are very different, even if they are generated immediately one from another. The encryption key for the components changes from one installer to other, although they tend to have the same key length for each campaign.

During our investigation, we were able to gather several samples of these tampered installers. The affected applications fall into several categories, such as application for compression like 7-zip and WinRAR archiver, security software such as McAfee Security Scan Plus, file recovery application - Recuva, application for remote connection such as TeamViewer, chat application such as WhatsApp or different tools and utilities like Piriform CCleaner, CleverFiles Disk Drill, DAEMON Tools Lite, Glary Utilities, or RAR Password Unlocker, covering a wide range of needs.

Each initial dropper has a compile time, the exact date the tampered installer was created. When we investigated this aspect, we observed that all the files we managed to retrieve were compiled from Monday to Friday, a normal work week. Another interesting aspect is that the time interval for these timestamps is around 9 hours, which is a workday norm. If we were to place this norm in a 9 to 6 working schedule the time zone would be UTC+2.





The above observation strengthens the idea that this threat is sponsored, and we are dealing with an organized developer team paid to work for this “project”.

The download server

While monitoring the threat actor activity, we were able to investigate several points from the infrastructure.

The download servers had some interesting particularities.

The actor has taken some security measures in order to ensure that only the “right” connections are accepted.

They use a helper script (self-named “Debian Stretch Hardening Script”) with the following help message:

```
usage: $0 options
Debian Stretch Hardening Script
OPTIONS:
-u Admin User
-p SSH Port
-k SSH Public Key (example : “ssh-rsa AAA...”)
-d Domain Name
-n Knock Ports (example : 10001,10002,10003,10004)
--helpHelp
```

The script, among other actions, updates all the packages, creates the “admin user” on the system (and computes the password for it, based on the Knock ports and SSH port), configures nginx and configures knockd service and the firewall. Due to an error in the script, the password is always the same. This does not represent a problem because the SSH daemon is configured to only allow public key authentication.

In one instance, the actor used a sequence of four Knock Ports when calling the script.

Interestingly, there seems to be a specific IP from Israel that is denied any connection to the download server, an IP address which seems to belong to an important science university.

Reviewing the software logic, we identified 2 directories with malicious binary files and 3 PHP scripts:

1. configuration.php – contains the locations of those 2 directories and a list named $targets (which should contain a list of IP ranges, but it is empty) and a mapping from 32 hex-digits to filename (which does not represent the md5 hash of the file, but uniquely identifies it- referenced from now on as file-id).
   - read.php – contains two functions:
   - checkUserIP() which checks if an IP address is contained in the $targets list
2. serveFile() – serve an installer file to the client
3. inject.php – the main logic. It Includes the other 2 php files, validates that the IP of the connecting client is among the targets list defined in configuration.php, checks the file-id and serves the chosen file.

According to the logic of the scripts, one of the directories should contain the original installers and the other the tampered ones. If the IP address of the victim is in the $targets list, a trojanized installer would be delivered, otherwise a legitimate one would be served. In the case of the nodes we investigated, both directories contained the exact same files and the $targets list was empty, meaning that any valid connection would get the malicious installer.

In the wild, we have seen the requests for the first layer of the following pattern:

`https://<download server>/<8 character folder>/<the 32 hex-digits that identify the file>`

But, in the nodes that we have analyzed, a valid URL would have the form:

`https://<download server>/<8 character folder>/<the inject.php file>?params=<the 32 hex digits that identifies the file>.`

This discrepancy points to either the nodes being out of use, or, the known URL scheme being changed.

Any other requests are redirected to https://google.com

Command and Control Servers

Once the malicious installer is downloaded and executed, the backdoor is installed. The backdoor will communicate with a command and control server, embedded into its binary, for document exfiltration and for retrieving commands to be executed, depending on the importance of the victim.

From an OPSEC point of view, the actor takes different actions in order to hide and anonymize its traces. The C2 network uses a set of proxy servers to hide the terminal node/nodes in the infrastructure. At the moment of writing, we have identified at least three layers in this infrastructure.

First layer

The first layer is made up of IPs to which the malware will try to connect. Each of these IPs has a unique domain associated to it that is embedded in the binary. These are in fact proxies to other machines.

The nodes we have seen use the PHP curl bindings to forward the request to the next server in the chain they know (one script for file exfiltration and one script for retrieving commands). If a node is compromised, one could not have details about the entire infrastructure, knowing only about the nodes before it and the node it submits data to.

The first layer does some basic validation and forwards the traffic to and from another server, which usually is located in a different country, at a different provider. The communication between the first layer and its upstream is HTTPS (the certificate is not verified) on an unusual TCP port for this protocol – 1402.

As for the software stack, nginx and php are used and configured to respond with 404 to all incorrect requests (either non-existing files, for which nginx serves the 404 response or for incorrect parameters to the PHP scripts, which falls into the php script's responsibility to serve the 404 code).

Second layer

The second layer is composed of the IP addresses that the first layer forwards data to. These IPs do not seem to have any domains linked to them and have multiple first layer IPs pointing to them.

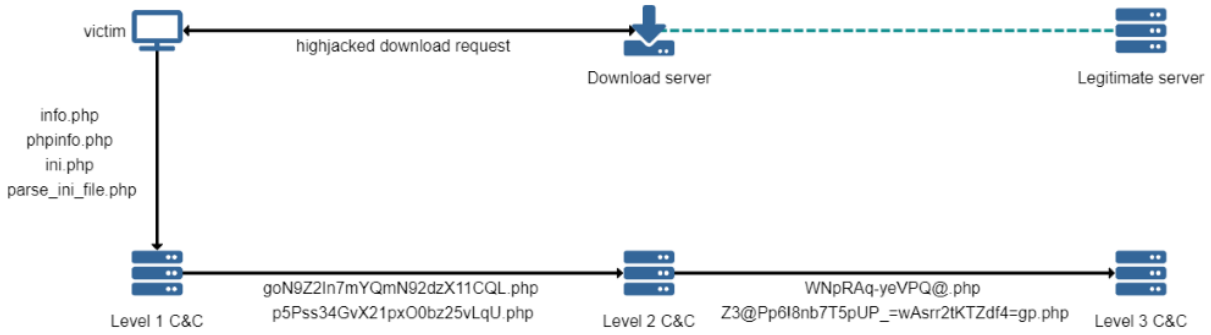
Other writeups mention the PHP scripts *goN9Z2In7mYQmN92dzX11CQL.php* (for file upload) and *p5Pss34GvX21px00bz25vLqU.php* (for getting the commands). These PHP files still exist in the whole infrastructure, but they now reside on the 2nd layer proxy, with the 1st layer/public facing script being named *info.php*or *phpinfo.php* (for file uploads) and *ini.php* or *parse_ini_file.php* (for the commands). The table below illustrates the names of these PHP scripts our researchers retrieved during the investigation on each layer from the infrastructure:

1st layer	2nd layer	3rd layer	Functionality
info.php phpinfo.php	goN9Z2In7mYQmN92dzX11C-QL.php	WNpRAq-yeVPQ@.php	file upload
ini.php parse_ini_file.php	p5Pss34GvX21pxO0bz-25vLqU.php	Z3@Pp6!8nb7T5pUP_=wAsr-r2tKTZdf4=gp.php	Get commands

Both the first and second layers have the SSH daemon configured to listen on a high port (bigger than 1024). By avoiding the use of the default port for a certain protocol, the threat actors are trying to ”stay under the radar” from common Internet scanners and search engines like Shodan or Censys.

As far as our researchers were able to investigate, the threat actors use a VPN service for connecting and administrating the servers , usually from secureconnect.me or torguardvpnaccess.com.

The figure below summarizes the communication between the proxy layers after an infection was performed:



In terms of infrastructure, we were able to map 47 servers with different functionalities. It does not seem that the threat actor prefers a particular hosting provider or region to set up the infrastructure, but most of them are in Europe.

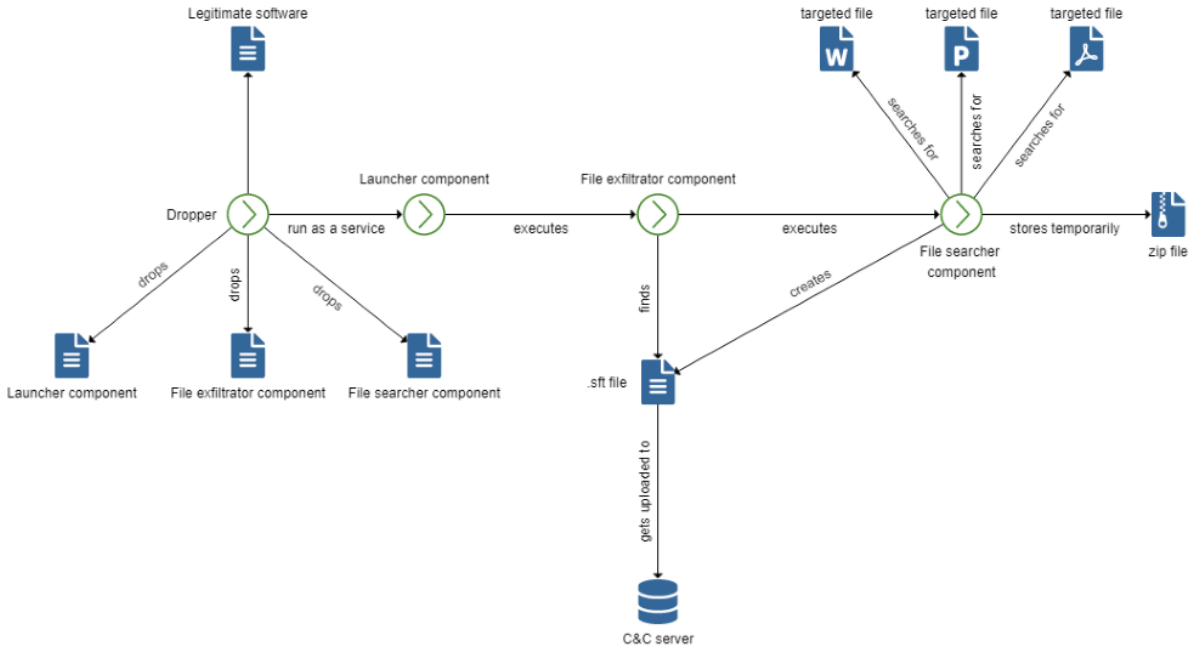
Components and Communication Protocol

Once the tampered installer is downloaded and executed, it will drop 4 files: the Legit Setup, the Launcher and Persistence component, the Exfiltration and Command Execution component and the File Searcher component.

The first executed file is the original installer, which will be prompted to the user so that they would not suspect anything. All malicious actions are performed in the background.

All of these 4 components are encrypted in the resource section of the initial dropper. Each resource has an 8-byte header that tells the dropper the size of the executable and the component type.

A summary of the installation process is illustrated in the figure below:



After the Launcher component is dropped into the %SYSTEM% folder, it is executed by calling the function responsible for creating a new service. The name of the service is a common one, either replacing a non-vital system service (***`Print Spooler`***) or having a name that does not raise any suspicions (***`Registry Maintenance Server`***). The service will be used as a persistence mechanism and will execute the Launcher component.

The dropper starts the service and will drop the rest of the executables.

The Launcher component executes the Exfiltration and Command Execution component, usually placed in the same system folder, and waits for an uninstall event.

The Exfiltration component is responsible for running the File Searcher component and for exfiltrating the files to the C&C server through a POST request. It regularly asks the C&C server for *download and execution* commands or an *uninstall* command. The last one, if received, will be sent as an event to the Launcher component. The *get_command* is sent as POST request with an argument called *name* that contains a tag. This tag is used as a form of authentication and is influenced by the compilation time of the file. In our tests, the servers always seem to respond with a 404 if asked for a command.

The File Searcher component loops through every drive and looks for files with certain extensions. The malicious binary has an extension list embedded (usually identifying different types of documents). If a file with an extension from that list is found, it will be copied into a temporary zip archive. After completing adding the files to the archive, it will split it

into hidden .sft encrypted files. The .sft files are read by the Exfiltration component, sent to the C&C server and deleted from the disk.

After the exfiltration process is completed, the Exfiltration component will wait for further commands as described above.

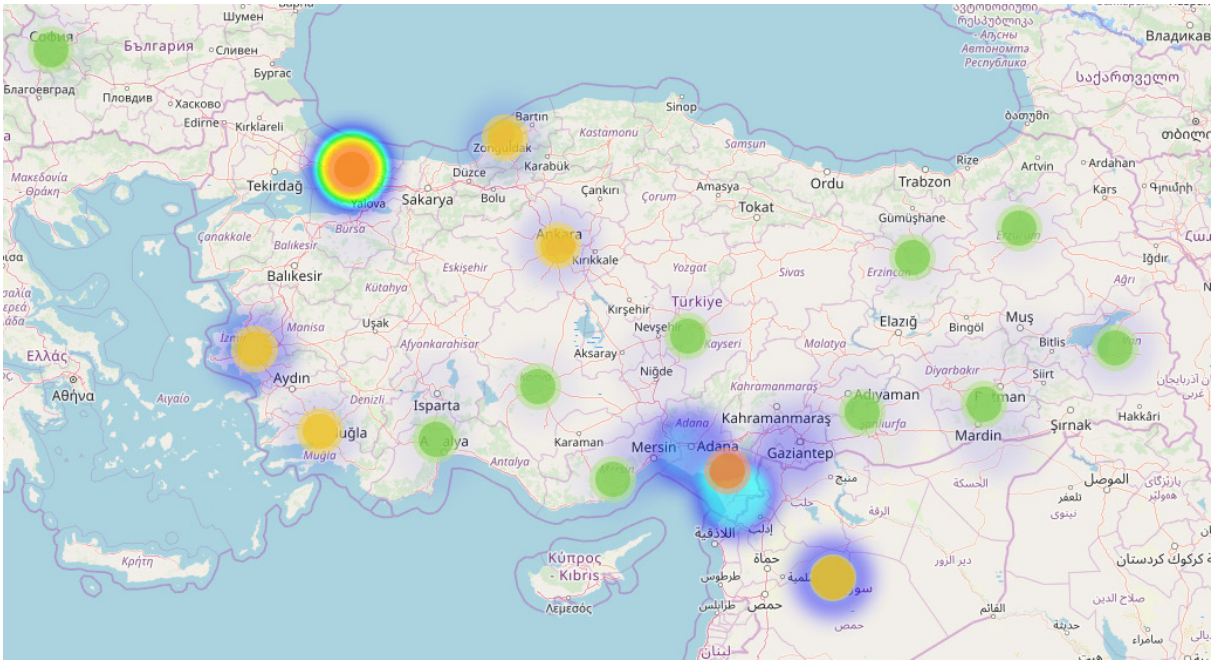
As mentioned earlier, the files that will be exfiltrated are first copied into a zip file. This zip file will be encrypted into multiple .sft files as follows:

- The File Searcher component will read 2048 bytes from the zip file
- For each byte it will apply a xor operation between the least significant 4 bits and the most significant 4 bits and it will write the result in the .sft file
- The first two steps are repeated a maximum of 53 times
- If the zip file still has unprocessed data, a new .sft file will be created
- For each zip file, the first .sft file will have a N prepended as a first character, the rest of the .sft files which complete an archive will have an O prepended.

Victims

While screening the victims it was obvious that this threat is an extremely targeted one. The majority of victims are concentrated in the area of Turkey and Syria.

Zooming in, we were able to observe that most of the targets are located near the border between Turkey and Syria, as well as in Istanbul, enforcing the idea that this threat might be involved in the geo-political conflict between Turkey and the Kurdish community.



Mitre Matrix TTPs

Initial Access	**Execution**	**Persistence**	**Defense Evasion**	**Credential Access**	**Discovery**	**Collection**	**Command And Control**	**Exfiltration**
Drive-by Compromise	Command-Line Interface	Hidden Files and Directories	Code Signing	Credentials in Files	File and Directory Discovery	Automated Collection	Commonly Used Port	Automated Exfiltration
Supply Chain Compromise	Execution through API	Modify Existing Service	File Deletion	Private Keys	Security Software Discovery	Data from Local System	Multi-hop Proxy	Data Compressed
	Service Execution		Hidden Files and Directories			Data from Removable Media	Multilayer Encryption	Data Encrypted
	User Execution		Masquerading			Data Staged	Standard Cryptographic Protocol	Data Transfer Size Limits
			Software Packing					Exfiltration Over Command and Control Channel

Appendix

Compile time	Hash	Tag
2/23/18 14:45	6189d3e23fd46225df49808af04acb93	v5_kt0_2526573066
2/23/18 14:45	68a7ec5cbc1d9829af68d049694e98d8	v5_kt0_2526573066
2/23/18 14:45	fb1891e4b5960bfbbe837456c142c474	v5_kt0_3162041892
2/23/18 14:45	196b09558ebc6df4f5e18f16dffd5dac	v5_kt6_3162041892
2/23/18 14:45	fff57c64bfe8c187f2bde0f285c4403d	v5_kt6_2526573066
2/23/18 14:45	5bfe33eacc0431f850e59c354ae379aa	v5_kt7_3162041892
2/23/18 14:45	f7712608ea96ede2b90092997c7b237d	v5_kt7_2526573066
3/27/18 7:45	fa4897922e8aef9317e750f9df3273e4	v5_kt10p2_2526573066
3/27/18 7:47	c765f756212b184fa1d7fef3da3ceda9	v5_kt24p2_2526573066
3/27/18 7:48	24660c650afbb338c549b0471668b84c	v5_kt31p2_2526573066
3/27/18 7:52	77d2a56d02e117d2e237999eab608297	v5_kt10p3_2526573066
3/27/18 7:55	0809b52c6d719e81b266eab49193a4fe	v5_kt25p3_2526573066
3/27/18 7:56	9f35b2ea6d8b99eea738a5c7b0f08f3b	v5_kt31p3_2526573066
3/27/18 8:21	b46ae605101ee411d8691286c7fd085b	v5_kt4p1_2526573066
4/9/18 12:41	5a939de0552b7b789ad7c776a3e0c4d5	v5_kt4p6_2526573066
4/9/18 12:41	66d84a8702313acd8f9d08fc3b8dad51	v5_kt4p6_3162041892
4/9/18 12:41	a92d2c37b6644d40477695c15c93252a	v5_kt4p6_3162041892
4/9/18 12:42	62ece27358e3eeb03dd746f3961be681	v5_kt10p6_2526573066
4/9/18 12:44	aa921b020c9923f4bb3ec70bcd307c4a	v5_kt24p6_2526573066
4/9/18 12:46	02cef69d95adbf58fc1f2dbbfbf8e522	v5_kt30p6_2526573066
4/9/18 12:46	d3a70def9f3ac3864a5535bf25ede8d0	v5_kt33p6_2526573066
5/15/18 13:58	29e323ae86a448e2a51cd6947074a615	v6_kt2p1_3162041892
5/15/18 13:58	3d39a210dd8b53ea403a0286805f9459	v6_kt2p1_3162041892
5/15/18 13:58	a7fb9e2061127f1e74c4d34df07d0d19	v6_kt2p1_2526573066
5/15/18 13:59	0f61cfa669e4f2711837b656d91775d7	v6_kt4p1_3162041892
5/15/18 13:59	18fd552a549f75c2798a760cac41717c	v6_kt4p1_3162041892
5/15/18 13:59	25ffb92e91b2865e961571d0ae0ca0db	v6_kt4p1_3162041892
5/15/18 13:59	e43d847aeda31ddd94fec050f4e887a9	v6_kt4p1_2526573066
5/15/18 13:59	f2e69eb169d4bacf26e7c4dc6dba3a93	v6_kt4p1_2526573066
5/15/18 13:59	fb64b106e15a98489834355509f4bb887	v6_kt7p1_2526573066
5/15/18 14:00	156f8752b9b46ac213d53970bd954aa1	v6_kt12p1_3162041892
5/15/18 14:00	8c13f1a357248b0eb5da35d11e2a8f4d	v6_kt12p1_2526573066
5/15/18 14:00	be5c5186ad6b0e503d1d5c664bd571f4	v6_kt12p1_3162041892
5/15/18 14:00	c9a141f5f3ff677611686605355c8eb0	v6_kt12p1_2526573066
5/15/18 14:02	39f9894b57db67c9090f24798e423575	v6_kt24p1_2526573066
5/15/18 14:03	4690cf81166147801ffe3226e7c619d0	v6_kt30p1_2526573066
5/15/18 14:03	cea2d61b1be9fc68da771a7d88f16ec6	v6_kt30p1_2526573066
5/15/18 14:04	9f6c3889e19cc7c9e0a09a8a12a65e77	v6_kt36p1_2526573066
5/15/18 14:04	2d3d2d277d9fdcb31f4ed07a12c7b578	v6_kt37p1_2526573066
5/15/18 14:04	4940c5a1ac1d04f47f17b3cafe7a53bb	v6_kt37p1_2526573066
5/15/18 14:04	98455706a66f7628101ee9d62ffca78d	v6_kt37p1_3162041892
5/15/18 14:04	464b0222ddeb613e91ea26e73aa716c1	v6_kt39p1_3162041892
5/15/18 14:04	69b5a2c62a1bbe121f039061e4e660aa	v6_kt39p1_2526573066
5/15/18 14:08	25ab473656ed395424a1c7db6717ab88	v6_kt0p2_2526573066
5/15/18 14:10	3c9061b7f93e2f96547959564211820f	v6_kt17p2_2526573066
5/15/18 14:10	bec13d67f1307c2d80861a20e5f41a71	v6_kt17p2_2526573066
5/15/18 14:13	06f259b09f22a1ef1d634a3c7f657e2f	v6_kt30p2_2526573066
5/15/18 14:14	58ba5b4383b56c4cf773cef65c107aa1	v6_kt37p2_2526573066
5/15/18 14:14	63a423c7785015c658c598af4d25a013	v6_kt37p2_2526573066
5/15/18 14:14	c37b8732fdf54e31d1788cc0b5b1f935	v6_kt37p2_3162041892
5/15/18 14:21	d04628fa29be5867003b95cbdc777918	v6_kt37p3_2526573066
5/15/18 14:21	f17def13d45cb90ce271c97703e5ca62	v6_kt37p3_2526573066
5/15/18 14:37	62476fd062f43b470997b5df1f1796bd	v6_kt17p5_2526573066
5/15/18 14:37	f02d4f48cd221015305758c51a0b9562	v6_kt17p5_2526573066
5/15/18 14:40	d5c2d195693c5b55436c26bf68106128	v6_kt30p5_2526573066
5/15/18 14:41	3e29cba37a988686990f7a38b2cf5a1c	v6_kt37p5_2526573066
5/15/18 14:41	ccb6b5ee662b64c127e4beba408a4e40	v6_kt37p5_3162041892
5/15/18 14:41	4502ccea6486ee1240a9a63a5ce3520c	v6_kt38p5_3162041892
5/15/18 14:41	f08b78775d5c68db5e5cf85346ed1771	v6_kt38p5_2526573066
5/15/18 14:41	fe305324ca36c922cbafdf12ed1916b1	v6_kt38p5_2526573066
5/15/18 14:45	c65e00f253dd93ea898eec3be9bf3e87	v6_kt4p6_2526573066

Compile time	Hash	Tag
5/15/18 14:45	f4831a0983e28ad14e16050e75893cb0	v6_kt4p6_2526573066
5/15/18 14:49	0629ab800ae234a056b8c3ee1b6d4e45	v6_kt29p6_2526573066
5/15/18 14:49	900d937455c62807fb4b0b0000142d37	v6_kt30p6_2526573066
5/15/18 14:50	4e01ec332c8b144bcd6e5b9336cd0515	v6_kt37p6_3162041892
5/15/18 14:50	600c9bb8464514e1ea71d7bae9c45f1b	v6_kt37p6_3162041892
5/15/18 14:50	74b5784591c2396ba9ee4be426d718d4	v6_kt37p6_2526573066
5/15/18 14:50	eaf857ca569edc8c82827c1411d6210b	v6_kt37p6_2526573066
5/15/18 14:50	fa1791c69ea88d9e59ef507b43f14b08	v6_kt37p6_3162041892
7/16/18 15:02	2d18af05c04e56ab513a06b0ae8bb40f	v7_kt16p1_2526573066
7/16/18 15:02	807618196117b66a0570aec6b319662f	v7_kt16p1_2526573066
7/16/18 15:02	e8c3d09c00195027121d2d94068133c1	v7_kt16p1_3162041892
7/16/18 15:05	812f7b14a5155bb9ce8ee2f6baab0f54	v7_kt28p1_2526573066
7/16/18 15:05	1e25c3f7b999d3245a9f8d129f65387b	v7_kt29p1_2526573066
7/16/18 15:07	016c627160e4d411f0f6983a1eea5433	v7_kt36p1_2526573066
7/16/18 15:07	33ed688a05c24ed0f298c4332d0f1c33	v7_kt36p1_2526573066
7/16/18 15:07	7f674307d603692fe0d1f9a904a6885d	v7_kt36p1_3162041892
7/16/18 15:07	9b72970d3d3708a3616f21bf913e6bd3	v7_kt36p1_3162041892
7/16/18 15:22	5922eed3d0ff4ac5d67aa154461be233	v7_kt4p3_2526573066
7/16/18 15:22	be668d459293f510ec4377f90b9ff288	v7_kt7p3_2526573066
7/16/18 15:23	d7e03a05f5c79a7d1fed4a01e068cede	v7_kt10p3_2526573066
7/16/18 15:23	6492bead898245869126ac93072f104e	v7_kt11p3_2526573066
7/16/18 15:23	6b0efa54601c0df5cc289805b78128f6	v7_kt11p3_2526573066
7/16/18 15:23	e24eca5fb3a3b39ca79a6e3d2c8638d6	v7_kt16p3_2526573066
7/16/18 15:25	a1acd72f9b55a50f32fcd0e14306eee6	v7_kt22p3_2526573066
7/16/18 15:26	08ac5e40dc2592d0829777ab2a390efd	v7_kt27p3_2526573066
7/16/18 15:27	155993907526f623d74caf3e629b88ac	v7_kt29p3_2526573066
7/16/18 15:28	3ddafc8e5c38d685e5036b4651e99734	v7_kt32p3_3162041892
7/16/18 15:28	b8e8828d3097b29e0c7c1638353d57a4	v7_kt32p3_2526573066
7/16/18 15:28	c4055e6fc86b515c1a0a0916a11392cc	v7_kt35p3_2526573066
7/16/18 15:29	05349edad0b996fb15625ec4177098a6	v7_kt36p3_2526573066
7/16/18 15:29	c35cf0170c05f38e19f57554b6f7c869	v7_kt36p3_3162041892
7/16/18 15:33	4ff4a7615ef5d17d200c20c19858512a	v7_kt16p4_2526573066
7/16/18 15:41	511f323b8fba0cee598a7e0f21cb67c8	v7_kt4p5_2526573066
7/16/18 15:41	71440e180bbae9fd1eb28e92f728e943	v7_kt4p5_2526573066
7/16/18 15:41	76da8035011b8e83e0a58ff114825867	v7_kt4p5_3162041892
7/16/18 15:41	a457f4ce44303fee4e3e0dceeba802eb	v7_kt4p5_3162041892
7/16/18 15:41	e973278a88d86abd790b95bbfcb05568	v7_kt4p5_3162041892
7/16/18 15:43	1689a51cbf961bb2c382578354616cd0	v7_kt16p5_2526573066
7/16/18 15:43	262fdd343a753420e6296894aa027715	v7_kt16p5_2526573066
7/16/18 15:43	f81bdb0cdcddff29cf8565dcb118762f	v7_kt16p5_3162041892
7/16/18 15:46	8662b9d612d2831c497886aa2b4f32eb	v7_kt29p5_2526573066
7/16/18 15:48	5414dd363495a0de2bf179891b9928d2	v7_kt36p5_2526573066
7/16/18 15:48	f29daa02dd362e1a5b4223ee0f365072	v7_kt36p5_2526573066
7/16/18 15:54	74d63e7991bed7522161da8fb00e2421	v7_kt10p6_2526573066
7/16/18 15:55	d24d6a359ea0083b43fd45ecb4eebefd	v7_kt16p6_2526573066
7/16/18 15:59	de30568e9166b924884c4f0262baf2ff	v7_kt29p6_2526573066
7/16/18 16:13	511325a99131b6598889229e15ebbbe0	v7_kt34p7_2526573066
10/22/18 9:08	6e5be93861b7041997e0ccd3d6a8b49f	v8_kt10p0_2526573066
10/22/18 9:08	1fefc3bf01c977005ef6a38e9cf5f0db	v8_kt11p0_2526573066
10/22/18 9:08	de5c56c01fcebbb23b496d3558377822	v8_kt11p0_2526573066
10/22/18 9:09	d07353df8ae524e951f98d25dd63303e	v8_kt16p0_2526573066
10/22/18 9:14	ce3010402ef522c3b7f5a6b840d5dc27	v8_kt27p0_2526573066
10/22/18 9:17	a5c8ec60e0985dd006e88540698307cc	v8_kt34p0_2526573066
10/22/18 9:17	bc4af9d40bcd6a355dbd974a970c3e72	v8_kt34p0_2526573066
10/22/18 9:20	59e2f2f37e18051470074ac3a027c3f6	v8_kt10p1_2526573066
10/22/18 9:20	f05586ee60c7c36410c558970dc5a538	v8_kt10p1_2526573066
10/22/18 9:22	a8ec5e46869747bfca8c5f8a93e9ba8e	v8_kt16p1_2526573066
10/22/18 9:22	b3ab9d4624af14d5adfdb98b9335a4b1	v8_kt16p1_2526573066
12/17/18 15:44	7146eff8308a6a9fb2ebb83c2377fb1e	v9_kt4p0_3162041892
12/17/18 15:44	897ee05e7ec8053ec5a1bf4d047abfac	v9_kt4p0_2526573066
12/17/18 15:44	efdba4cc90f118766fe78b60e92d56c9	v9_kt4p0_2526573066
12/17/18 15:44	f6d57949803a65ca1ed6f9544e1a2796	v9_kt4p0_3162041892
12/17/18 15:46	454ad5b7a1f9e7e36dc7742b8fb5c62a	v9_kt17p0_2526573066
12/17/18 15:46	a05199b00edd8faa714493bb91e55176	v9_kt17p0_3162041892
12/17/18 15:46	a540d3fac2aac67d86adf674ed0a9fd8	v9_kt17p0_2526573066
12/17/18 15:47	79b11e614fe7922ab24044315cc2782a	v9_kt21p0_2526573066

Compile time	Hash	Tag
12/17/18 15:47	d84443aea0cc4ddfe1386e4653649cab	v9_kt21p0_3162041892
12/17/18 15:51	07f43cc57f7f1cba27aea5dd972ff20d	v9_kt38p0_2526573066
12/17/18 15:51	5ef12a07d84f5e5ab152d55777ec4635	v9_kt38p0_3162041892
12/17/18 15:51	9b83cd27cae041c8d9de8743cdf0d045	v9_kt38p0_3162041892
12/17/18 16:09	2b2f7890f15545ad946942fede3d8c19	v9_kt4p3_3162041892
12/17/18 16:09	f9553abcb9b2ef39478f483e13e1a0e7	v9_kt4p3_2526573066
12/17/18 16:18	3dcab377355ba96b85569db086c4d1e9	v9_kt8p4_2526573066
12/17/18 16:18	50b58036440e5b4c702ff57dcf979726	v9_kt8p4_3162041892
12/17/18 16:18	7d33236029aee1b25ed9661858102703	v9_kt8p4_2526573066
2/4/19 10:15	76d116964a9d15c2e14963d5f286eef5	v10_kt4p0_2526573066
2/4/19 10:15	9e89e681b3fcb9d7b5614c6f3f14bbe8	v10_kt4p0_2526573066
2/4/19 10:15	d1eb79451c98194a81955a66ea7d15d8	v10_kt4p0_3162041892
2/4/19 10:15	156f39ec94bd95334ecf639dd1489927	v10_kt8p0_2526573066
2/4/19 10:17	ee1d7e6fa9faf2097d84a0dde2848435	v10_kt15p0_2526573066
2/4/19 10:17	2062c64ddb1ee195aa4564fa52b9842b	v10_kt17p0_2526573066
2/4/19 10:17	956b667fd0717280ac428135bfd1a5fb	v10_kt17p0_2526573066
2/4/19 10:18	12305660ba6c79a74cd5aee9e7355829	v10_kt21p0_2526573066
2/4/19 10:18	18ff702d36348a0bc1fd25b177616284	v10_kt21p0_2526573066
2/4/19 10:19	0dfb7413456d1ac1080431e6d85ad5b5	v10_kt34p0_2526573066
2/4/19 10:19	9798f0f65026e44b94851938dc68b296	v10_kt34p0_2526573066
2/4/19 10:21	196e30e9367bf7c094c6546c46a5ddac	v10_kt38p0_2526573066
2/4/19 10:21	55e60a488b5abc6bb7d4a7ac201ec34a	v10_kt38p0_2526573066
2/4/19 10:21	6cfe9e4482cdbe87c3b8635d625e74f4	v10_kt38p0_3162041892
2/4/19 10:21	c0ec2596d5be34db2d225647da876ff6	v10_kt38p0_3162041892
2/4/19 10:21	7b7f472f2665851a61b72fd855826bfc	v10_kt40p0_3162041892
2/4/19 10:21	e4c5fe637b0ad8b28c195c3f04f40a40	v10_kt40p0_2526573066
2/4/19 10:21	0a3c01ccd948ec12d75cb591ab320887	v10_kt41p0_2526573066
2/4/19 10:21	17ab6936b3947a729613461b210aeff3	v10_kt41p0_3162041892
2/4/19 10:21	621748655953364c14462833ffaeca2b	v10_kt41p0_2526573066
2/4/19 10:26	51c1d0c4d3a0bd6505e268777ad994d6	v10_kt22p1_2526573066
2/4/19 10:26	bdc20cb24455e6a25548553daacc450e	v10_kt22p1_3162041892
2/4/19 10:26	d83acb06ec640abbce2b1f550c86bc2d	v10_kt22p1_3162041892
2/4/19 10:42	26ae59318dbca2747b479bad35a9f1a2	v10_kt21p3_3162041892
2/4/19 10:42	3cae6944adb9a2bf48eedc03e19fde8a	v10_kt21p3_2526573066
2/4/19 10:42	7b01de3ba7a1f91941210328b52aef2a	v10_kt21p3_2526573066
2/4/19 10:43	08f8dbc010ec24fa565c4edfd1d53d05	v10_kt27p3_2526573066
2/4/19 10:43	0b5c01152b6b52dd507c6056f13e8f7a	v10_kt27p3_3162041892
2/4/19 10:45	e935327bef67d8bfc2df5697e103eac7	v10_kt38p3_2526573066
2/4/19 10:45	ff044850564ed93534914e74745b2021	v10_kt38p3_3162041892
2/4/19 10:47	f0b01b999f34fd3c576f025ea7d5f209	v10_kt8p4_2526573066
2/4/19 10:49	c5c5a751c63ef4cdd6bfd34780068f00	v10_kt17p4_2526573066
2/4/19 10:49	fa0a842cb3ad4ed92dc583e108c47fd6	v10_kt17p4_2526573066
2/4/19 10:50	2109b47b30115cbd1ed05b8773672a6b	v10_kt21p4_3162041892
2/4/19 10:50	45880c5da170a3440ad8426fbbdcf48b	v10_kt21p4_3162041892
2/4/19 10:50	55dc3aa632efe8b2b0d21edaf284d9ad	v10_kt21p4_2526573066
2/4/19 10:50	a584016075493d2f6cbfeb4c2138027f	v10_kt21p4_3162041892
2/4/19 10:50	d0d2442edc79ab695d86da6e6aff496f	v10_kt21p4_2526573066
2/4/19 10:54	1dbd77469733bdd2c93b0879b62e0eff	v10_kt41p4_3162041892
2/4/19 10:54	d203834260cdd31a0b585f5dd56f6c55	v10_kt41p4_3162041892
2/4/19 10:54	d79f8aed9248a5be169fe59e2ca4a54f	v10_kt41p4_2526573066
2/4/19 10:54	e10b330a286b4646514a4131a90ad0cf	v10_kt41p4_2526573066
2/4/19 11:22	8dfba1f6931faeacd0d65841db8ecd9e	v10_kt21p8_2526573066
2/4/19 11:22	ce7161ca4fc79cd03bfbeec61339ebac	v10_kt21p8_3162041892
2/4/19 11:26	234882f8b4db2f42ff2cb3cad340ad9f	v10_kt38p8_2526573066
2/4/19 11:26	4542c8ee4e61edb2401bfb50539595a2	v10_kt38p8_3162041892
5/21/19 13:55	a4d3b78941da8b6f4edad7cb6f35134b	v11_kt5p0_2526573066
5/21/19 13:55	bb81f3cce7429b5bfcfedfee195a8132	v11_kt5p0_2526573066
5/21/19 13:56	2003f9a22bde7afbe7824918f78ccbf0	v11_kt6p0_2526573066
5/21/19 13:56	242ce2ce36874bccbf526f097e18d8f7	v11_kt6p0_2526573066
5/21/19 13:56	95c7a3553570c6dca6910c38eb0c3822	v11_kt6p0_3162041892
5/21/19 13:58	2d0f3620bbea500e7cfab2f28fb10e9b	v11_kt16p0_2526573066
5/21/19 13:58	d5669d903afccecfea9768d6fc6ad0e9	v11_kt16p0_2526573066
5/21/19 14:00	55bed06ad7f816e537ce83cc04a43971	v11_kt24p0_2526573066
5/21/19 14:02	6cdd4a2f81f453c478cf08c4d60cb88e	v11_kt26p0_2526573066
5/21/19 14:02	a2ac79ba2da6c41dad61af89b02cd786	v11_kt26p0_3162041892
5/21/19 14:02	c6fac70cd16a4a22e5670bfcff362098	v11_kt26p0_3162041892

Compile time	Hash	Tag
5/21/19 14:02	fb623ec504bb3864d786741d74d435f8	v11_kt26p0_2526573066
5/21/19 14:02	05e373b594b9995dbc876fba21e1a082	v11_kt28p0_2526573066
5/21/19 14:06	394551ee3214828bc92e43103931ff91	v11_kt16p1_2526573066
5/21/19 14:06	64e97f87968bc3696ac453b6ea1c19c8	v11_kt16p1_2526573066
5/21/19 14:23	257675532b975e1a3aba490056555d20	v11_kt16p3_2526573066
5/21/19 14:24	133bc4716ab72c5f238ad689b06a406e	v11_kt19p3_3162041892
5/21/19 14:24	215e6dcc8f83070c52dc45a88bf9f300	v11_kt19p3_2526573066
5/21/19 14:24	470221d850861c043d18dcda4be5bf7d	v11_kt19p3_2526573066
5/21/19 14:26	0d7357c3a2d878336adcd047e38cb6ac	v11_kt26p3_3162041892
5/21/19 14:26	0ec51113584217eba24e41698a3511a7	v11_kt26p3_2526573066
5/21/19 14:26	e8519538a8b8a319c617caaa5d8f5dc0	v11_kt26p3_2526573066
5/21/19 14:31	96d7b5b4972e51046f5ee45c74ecf134	v11_kt16p4_2526573066
5/21/19 14:31	ce17d73bd8567922a5570bd2ba437f27	v11_kt16p4_2526573066
5/21/19 14:32	7406709c1e9be859995fe5e6c7d2892b	v11_kt19p4_2526573066
5/21/19 14:32	e9b03320f643cc7252938b77c89c4092	v11_kt19p4_2526573066
5/21/19 14:35	4558c7d8be4ec2e05c9de809ef882bd1	v11_kt26p4_2526573066
5/21/19 14:35	788ca10ae955b9d3aecd8ba501a72291	v11_kt26p4_2526573066
5/21/19 14:35	0786cb5d49c0c80e655d72ecbbc8c4cb	v11_kt28p4_2526573066
5/21/19 14:38	a0f14f5d0f833dfa2a99220befc2fa84	v11_kt13p5_2526573066
9/18/19 9:51	ad2c4fc5d470fa0c238afdc821080d4c	v12_kt20p2_2526573066
9/27/19 11:52	2500f9b20567ee062c4cd03ef4093b18	v12_kt30p8_2526573066
10/1/19 13:40	09c55dbda0004fd7e048bdd910e909b4	v12_kt0p9_2526573066
10/1/19 13:41	4c14dc8e5f21c6376d8e8a3a73523f4e	v12_kt1p9_2526573066
10/1/19 13:41	c99b6d13a27102a3bca2d625bb7a676c	v12_kt2p9_2526573066
10/1/19 13:41	3b1482dbfd318fd60e32fbcd972d6d73	v12_kt3p9_2526573066
10/1/19 13:43	c6e68619fcf40ecd8346963ddf2c0d68	v12_kt4p9_2526573066
10/1/19 13:44	0201b7cee2af2bd453db5673de6ba792	v12_kt5p9_2526573066
10/1/19 13:45	ccf61707157bec61709391daa014694d	v12_kt6p9_2526573066
10/1/19 13:46	4634885a7ea08194d22b13ee2448c32e	v12_kt7p9_2526573066
10/1/19 13:46	a8341ac6c2e1b230d4b861cb9ee57b11	v12_kt8p9_2526573066
10/1/19 13:46	0f86cdd03af65f38f0fad59f527f609e	v12_kt9p9_2526573066
10/1/19 13:47	81dc8d83a3d8cbec17ff79f0510b248e	v12_kt10p9_2526573066
10/1/19 13:47	1c32104eb2bd9c102256212bd033d145	v12_kt11p9_2526573066
10/1/19 13:47	627493950411f37a55012374da6d0133	v12_kt12p9_2526573066
10/1/19 13:48	25987155b8908d9d9e70966864e5bf5b	v12_kt13p9_2526573066
10/1/19 13:48	0c6fbcb537644cb29a66163c3ea28cce	v12_kt14p9_2526573066
10/1/19 13:49	7cb5c95f203346cd5f1a02a05df840bb	v12_kt15p9_2526573066
10/1/19 13:49	03df5ff14c51cb7fc0410016a0a59054	v12_kt16p9_2526573066
10/1/19 13:50	5e689fa90834164e176806fda59dfcbe	v12_kt17p9_2526573066
10/1/19 13:51	49d7a905da87f80bd86f16353aa0b2bd	v12_kt18p9_2526573066
10/1/19 13:52	b32ef1b7c01a6ba2513fc68b838e2ebc	v12_kt19p9_2526573066
10/1/19 13:52	b17c845e47fb3b825729e8499e0feb3c	v12_kt20p9_2526573066
10/1/19 13:53	ab16fd949da9da58532e2d7df3a561ac	v12_kt21p9_2526573066
10/1/19 13:53	1803953d76c9259acd2c8f3d38e2821d	v12_kt22p9_2526573066
10/1/19 13:54	1429a22a0d69b729c4ec993b48f381ed	v12_kt23p9_2526573066
10/1/19 13:55	563a3d500e05ee2cd09a277656ed14b9	v12_kt24p9_2526573066
10/1/19 13:56	cbc5605106414a55c5837b53fc8d5efd	v12_kt25p9_2526573066
10/1/19 13:56	6d28901b2998c047a98ab7848f68ac45	v12_kt26p9_2526573066
10/1/19 13:56	8dd3003e534d596bd371eb1b592c809a	v12_kt27p9_2526573066
10/1/19 13:57	b645e18e5b9f772c4dbf0e9e97d201d6	v12_kt28p9_2526573066
10/1/19 13:57	2c21ee9b69b945499f060c82b583c5f2	v12_kt29p9_2526573066
10/1/19 13:57	f382f743c5397f07f88e5983748b220f	v12_kt30p9_2526573066
10/1/19 13:57	36197b90d8f55982c4d9d95eb3a98196	v12_kt31p9_2526573066
10/1/19 13:58	806e9f175a9506905600a5a959d5b131	v12_kt32p9_2526573066
10/1/19 13:59	2ca19482de35dc87eed32b477d4aa693	v12_kt33p9_2526573066
10/1/19 14:00	51801197da6f0a4b26a85050d5834d8b	v12_kt34p9_2526573066
10/1/19 14:01	16aad4acaaf91732da1cdb889abfa095	v12_kt35p9_2526573066
10/1/19 14:02	8c7adb2ebe8504d5a16c69541dda018f	v12_kt36p9_2526573066
10/1/19 14:02	66881aedeee639cb83907ac3fe4bf6bc	v12_kt37p9_2526573066
10/1/19 14:02	6e934f3c024903b7bbeaec714133af8b	v12_kt38p9_2526573066
10/1/19 14:02	e39f6958f115d56f0e92722c3be52dc7	v12_kt39p9_2526573066
10/1/19 14:03	5745e2f15c73da6051f66b85be3f8092	v12_kt40p9_2526573066
10/1/19 14:03	6cdce7013ee3ee39d9cb03ecda78e386	v12_kt41p9_2526573066
10/1/19 14:03	5e197e21c6f108ca3f813197c901ca11	v12_kt42p9_2526573066
10/1/19 14:03	cf0c660bad1c629e875520078d719655	v12_kt43p9_2526573066
10/1/19 14:04	60eb3c75cd3bc5646101b7fd85754fec	v12_kt44p9_2526573066

Compile time	Hash	Tag
10/1/19 14:05	5e38caab88982a481be5cbe0874a19a5	v12_kt45p9_2526573066
10/1/19 14:05	03ca6b15114543a2e0ec21fe8f3ece26	v12_kt46p9_2526573066
10/1/19 14:05	0fd7b2982704308297e336bba75cf4fb	v12_kt47p9_2526573066
10/1/19 14:05	1efa229de68b78cf5ef730f422aca6e3	v12_kt48p9_2526573066
10/1/19 14:06	9715a5ba85c5712c420f23a21d233e98	v12_kt49p9_2526573066
10/1/19 14:06	9d775bb43de101f2813a5f63e3d984b1	v12_kt50p9_2526573066
10/1/19 14:06	ffc1af60f64aad6432be15f1b2a51f5a	v12_kt51p9_2526573066
10/1/19 14:07	5084515828f2d6ade3d97db915913125	v12_kt52p9_2526573066
10/1/19 14:07	8de397c6810f118f276dca54de01b42d	v12_kt53p9_2526573066
10/1/19 14:09	ba8deb03b22bda5c2fe29b610b000de1	v12_kt54p9_2526573066
10/1/19 14:10	aaf0ab461faba3820173799f98d63741	v12_kt55p9_2526573066
10/1/19 14:10	0c369c59167843a942149f704f573f24	v12_kt56p9_2526573066
10/1/19 14:10	bdd7404d410670639c3c3fa804952c1a	v12_kt57p9_2526573066
10/1/19 14:11	16129e6c855310ca95a8811fbbcf9008	v12_kt58p9_2526573066
10/1/19 14:11	6c1f4d7d0842d855ab8eda52c70113a9	v12_kt59p9_2526573066
10/1/19 14:11	eb9f1efa390cdd12c91a94a33848b22f	v12_kt60p9_2526573066
10/1/19 14:11	1bcf111f0d037b5b3204f8f34ee6a511	v12_kt61p9_2526573066
10/10/19 10:41	d7b7c35671bf793c2cf4a651fa86e748	v13_kt10p0_2526573066
10/10/19 10:48	cab76ac00e342f77bdfec3e85b6b85a9	v13_kt33p0_2526573066
10/10/19 10:52	31c7ff354b4b64c34223b90b06cbac65	v13_kt48p0_2526573066
10/10/19 10:55	564200f8b4e5469d2b1367e9722208cb	v13_kt57p0_2526573066
10/10/19 11:20	6ff8b82cba640ba3bebaa9172f88836b	v13_kt21p2_2526573066
11/4/19 13:57	99a09cf1a4c4799597f355a9dbe3c813	v14_kt16p0_2526573066
11/4/19 14:00	b23adfdeae37684b0e79a94790c96589	v14_kt24p0_2526573066
11/4/19 14:10	743f336ac73bf777429d451df6cd20de	v14_kt43p0_2526573066
11/4/19 14:22	4f6d3ef07f3cbeb61d038f339440c32c	v14_kt24p1_2526573066
11/4/19 14:28	c4feb0857787413da6b2e67f6c4e0738	v14_kt36p1_2526573066
11/4/19 14:41	7c5951f7b31070f0bfabf04ca6bc7949	v14_kt14p2_2526573066
11/4/19 15:04	b7677e42852e9b8a3857476fda540224	v14_kt16p3_2526573066
11/4/19 15:12	17f8871e99cb456eb8a4dbb3f1d6bbbc	v14_kt33p3_2526573066
11/4/19 15:19	9db8a8c98f18bcdca3037ab4d1b161e0	v14_kt48p3_2526573066
11/28/19 8:22	fabd81db6ca12ea6a5d43807a467fc4e	v14_kt15p4_2526573066
11/28/19 8:22	5f0913855b2772e65e36f98fbb48673d	v14_kt17p4_2526573066
12/12/19 7:31	1dc4268197f4bf6f99cdf1635735a605	v15_kt7p0_2526573066
12/12/19 7:31	80737d1e7b7d104635cb3421a76d2649	v15_kt10p0_2526573066
12/12/19 7:38	abca4446d9af5c4b91b7aa555ed0afb4	v15_kt26p0_2526573066
12/12/19 8:31	5305b70670b1f627b6801e762f5de2af	v15_kt76p1_2526573066
12/12/19 8:47	80a22aa0b3a46905d8b3ac9aae365d1b	v15_kt36p2_2526573066
12/12/19 8:54	08b2d8f653f6c2dedcb27897a3d56d18	v15_kt56p2_2526573066
12/12/19 9:42	dd0cdbf78966a41e064daf490f95ceaa	v15_kt16p4_2526573066
12/12/19 9:42	73faf13cbf33e00d730a6b9a00cb277e	v15_kt17p4_2526573066
12/12/19 9:43	7000b0c5e5f86a04c78375e566143ef8	v15_kt19p4_2526573066
12/12/19 9:49	9a91c808a447e33891db5282decc8a14	v15_kt33p4_2526573066
12/12/19 10:06	e4758783b146b506e0ec42e98ad9e65c	v15_kt70p4_2526573066
12/12/19 10:15	a9c7d342359cb7a6180f71c6dc18be2b	v15_kt20p5_2526573066
12/12/19 10:24	ab6d150d745053afae1d86f464954c42	v15_kt42p5_2526573066
1/23/20 9:50	6638cbb2f3c00eaa37faac6952aec795	v16_kt55p2_2526573066
1/23/20 10:04	d9cdbdaa8887140882a14fa3b25667fe	v16_kt7p3_2526573066
1/23/20 11:24	42f9375f6d99d92955766edf5aa6f88a	v16_kt32p5_2526573066

Why Bitdefender

Proudly Serving Our Customers

Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as **Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems** place in us.

Leader in Forrester's inaugural Wave™ for Cloud Workload Security

NSS Labs "Recommended" Rating in the NSS Labs AEP Group Test

SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row

Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20.000 Worldwide Partners

A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN's Security 100 List. CRN Cloud Partner, 2nd year in a Row

More MSP-integrated solutions than any other security vendor

3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority

Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.**

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

TECHNOLOGY ALLIANCES

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-PR-Whitepaper-StrongPity_APT-creat4574-en_EN
06/15/20June 15, 2020 12:19 pm06/15/20