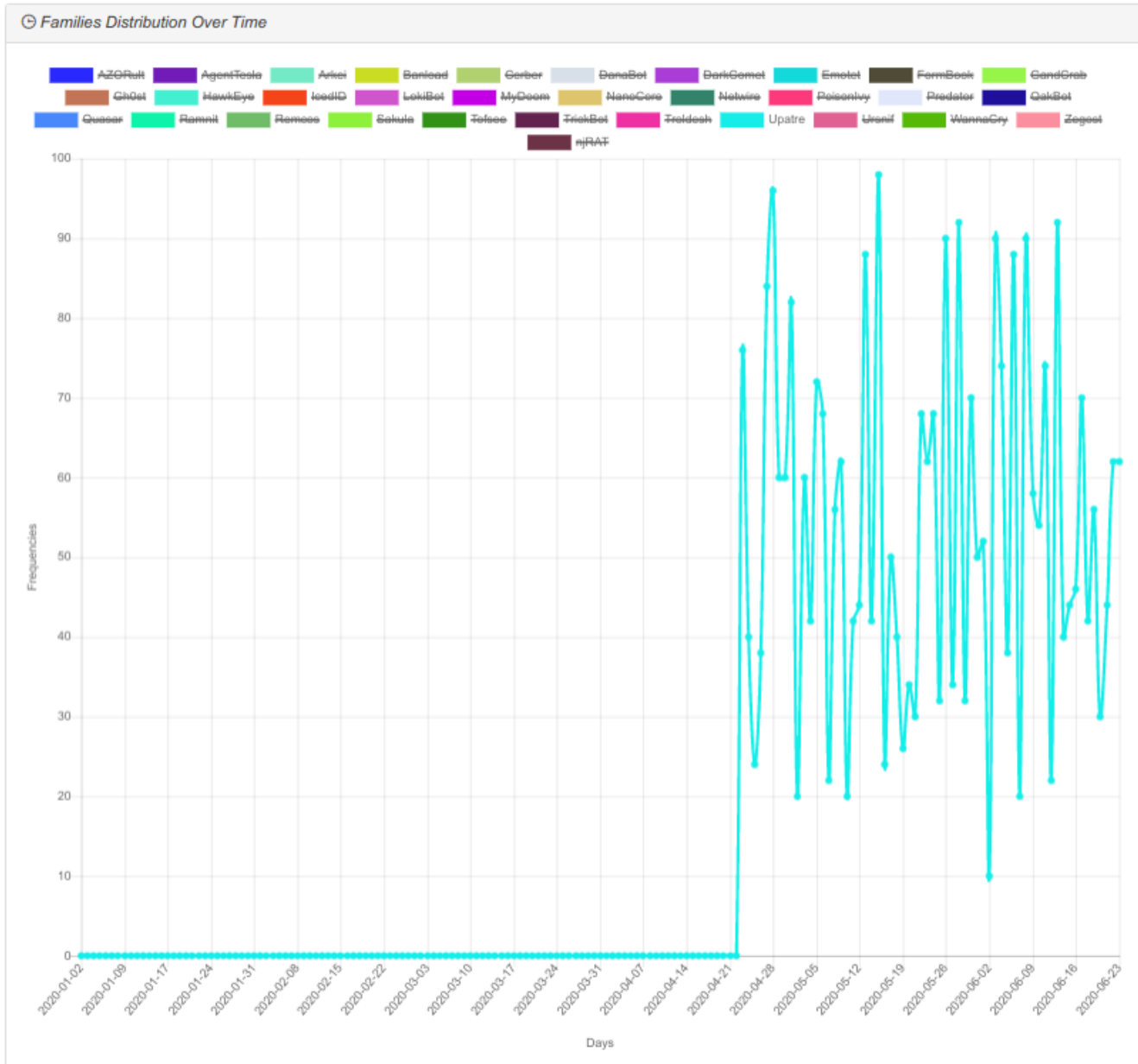


Is upatre downloader coming back ?

marcoramilli.com/2020/06/24/is-upatre-downloader-coming-back/

View all posts by marcoramilli

June 24, 2020



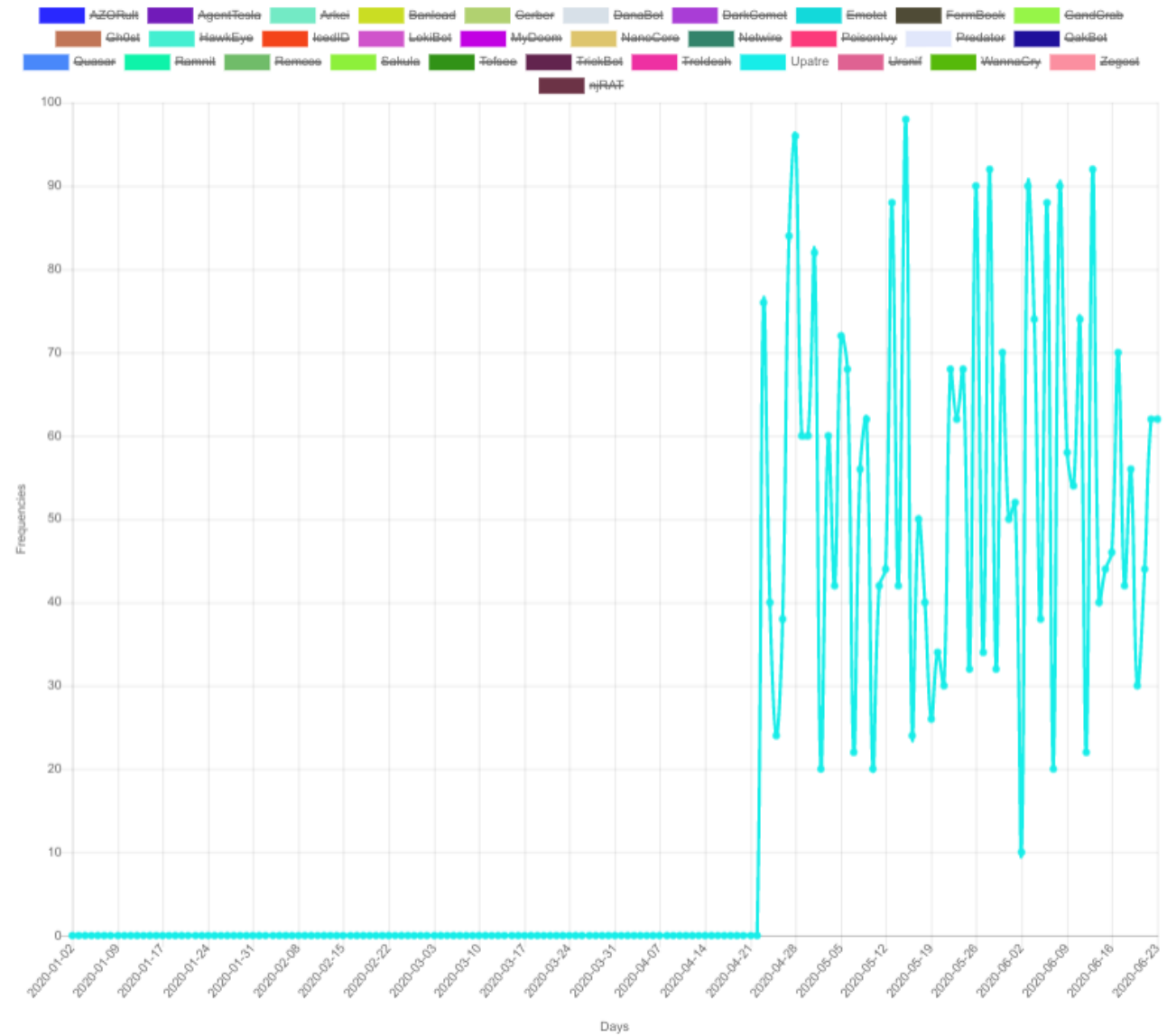
Hi Folks, today I want to share a quantitative analysis on a weird return-match by **Upatre**. According to Unit42 Upatre is an ancient downloader firstly spotted in 2013 used to inoculate banking trojans and active up to 2016.

First discovered in 2013, Upatre is primarily a downloader tool responsible for delivering additional trojans onto the victim host. It is most well-known for being tied with the Dyre banking trojan, with a peak of over 250,000 Upatre infections per month delivering Dyre back in July 2015. In November 2015 however, an organization thought to be associated with the Dyre operation was raided, and subsequently the usage of Upatre delivering Dyre dropped dramatically, to less than 600 per month by January 2016.

From PaloAlto Unit42

From 2016 until today I've never experienced a new Upatre campaign, or something like that, but something looks to be changed. Analyzing the [Cyber Threats Trends](#) findings (for an upcoming post) I spotted an interesting revival of the **Upatre** downloader starting from **April 2020**. The following image shows what I mean. Zero Upatre findings until April 21 2020 and almost 50 single detections per day since that date. Those statistics are so strange to me, that I need to doubt about that. So let's take a closer look to it and see if there is some misclassification around.

Families Distribution Over Time



Upatre Time Distribution

Digging a little bit on that samples by asking a second opinion to VirusTotal it looks like matches are genuine. In order to verify that “revival”, I firstly have taken some random samples (with Upatre classification tag) and then verified on VirusTotal the malware classification and the first submission date. Following an example of the performed checks. As you might see from the following picture, 9 AV classified that sample as Upatre, so we might consider not a “false positive” or a “miss-classificated” sample.

Engine	Detection	Engine	Detection
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Trojan.Upatre
MAX	Malware (ai Score=88)	MaxSecure	Trojan.Upatre Gen
McAfee	GenericRXIH-MAI89C0BFFD5B4A	McAfee-GW-Edition	BehavesLike.Win32.Backdoor.cz
Microsoft	TrojanDownloader.Win32.Upatre	NANO-Antivirus	Trojan.Win32.Dwn.duffvj
Panda	Trj/Genetic.gen	Rising	Malware.FakePDF@CVI1.A24A (RDMK...
Sangfor Engine Zero	Malware	SentinelOne (Static ML)	DFI - Malicious PE
Sophos AV	Mal/Vawtrak-S	Sophos ML	Heuristic
SUPERAntiSpyware	Trojan.Agent/Gen-Malagent	Tencent	Malware.Win32.Gencirc.10b8f176
Trapmine	Malicious.high.ml.score	TrendMicro	TROJ_UPATRE_SMJTU
TrendMicro-HouseCall	TROJ_UPATRE_SMJTU	VBA32	TrojanDownloader.Upatre
VIPRE	Trojan-Downloader.Win32.Waski.mf (v)	Webroot	Trojan.Downloader.Gen
Yandex	Trojan.Agent!gR8lkmctutg	Zillya	Downloader.UpatreGen.Win32.70

Upatre Correct Classification

The following image shows the “First Submission Date” which is aligned to what I’ve seen on [Cyber Threats Trends](#). If you take some more samples from the following list (IoC Section) you will probably see much more cases similar to that one. I did many checks and I wasn’t able to find mismatches at all, so I decided to write up this post about it.

61 / 72
61 engines detected this file

6238cf20bb8ea33986554eeefb0ac6947af1406c2ec57a72a378582a5625e3d71
ucedhafa.exe | 128.30 KB Size | 2020-04-19 19:53:43 UTC 2 months ago

direct-cpu-clock-access | overlay | peexe | runtime-modules

Community Score: 61 / 72

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Basic Properties

MD5	89c0bfd5b4aac3efbc754d8522189d
SHA-1	b7a79d50bb163965f2ac217b18d7a713d0d6d5b3
SHA-256	6238cf20bb8ea33986554eeefb0ac6947af1406c2ec57a72a378582a5625e3d71
Vhash	015056551d155417z20031nz55z17z
Authentihash	188805130bd98605a2f806cbe7ee828a026300b644e8dd5420de3cce528477
Imphash	f9e96ebb8d34f0e22d985ef2bd03cc45
SSDEEP	768:unmdSjy1/UhAorJNiXn0GGgJKDhwwznVN8p4/c1Z1C0vPH7mgvqq:unfe1VorJNE0GGgAhwAtVN8KuCqHnp
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	128.30 KB (131382 bytes)
PEID packer	Microsoft Visual C++

History

Creation Time	2015-07-20 09:54:13
First Submission	2020-04-19 19:53:43
Last Submission	2020-04-19 19:53:43
Last Analysis	2020-04-19 19:53:43

Upatre First Submission

Conclusion

It's something very interesting, at least to my understanding, to see an ancient downloader be resumed in such a specific period. Many people starting from April up to today are stuck at home performing what has been called "quarantine" due to COVID pandemic. Curiously during the same time, while people are working from home and potentially have much more free time (since they can't get out home), this older downloader reappears. Maybe somebody took advantage from this bad situation to resurrect some old tools stored in dusty external hard-drive ?

IoC (3384)

For the complete IoC list check it out: [HERE](#)