Curated Intelligence

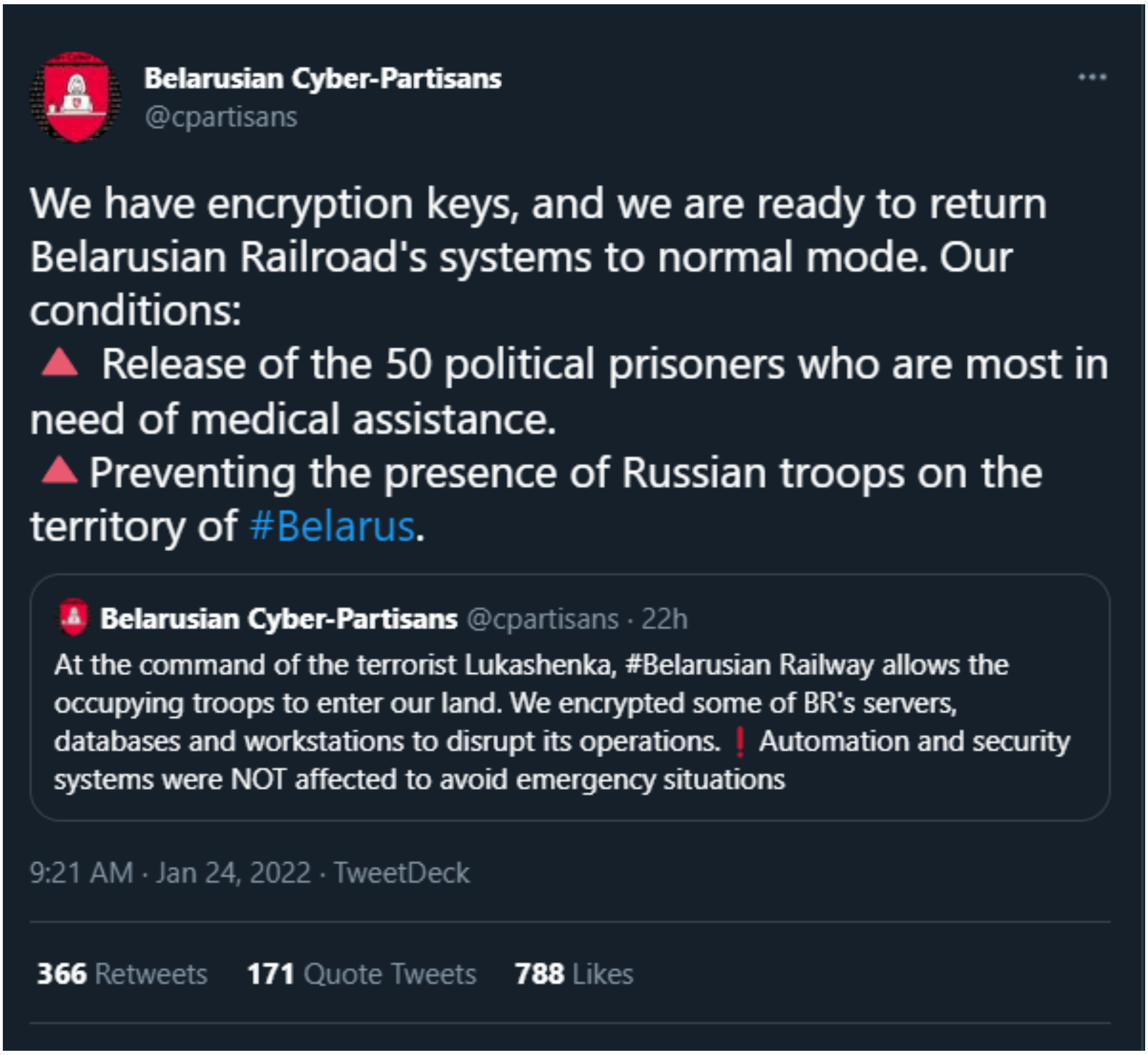
Hacktivist group shares details related to Belarusian Railways hack

January 25, 2022

The Belarusian Cyber Partisans have shared documents related to another hack, and explained that Curated Intel member, SttyK, would "understand some of the methods used."

Written by @BushidoToken and edited by @SteveD3

On Monday 24 January 2022, a Belarusian hacktivist group going by the name Belarusian Cyber-Partisans claimed responsibility for a limited attack against the national railway company. A primary objective of the attack, they claimed, was aimed at hindering Russian troop movements inside Belarus.



Belarusian Cyber-Partisans
@cpartisans

We have encryption keys, and we are ready to return Belarusian Railroad's systems to normal mode. Our conditions:
🔺 Release of the 50 political prisoners who are most in need of medical assistance.
🔺 Preventing the presence of Russian troops on the territory of #Belarus.

Belarusian Cyber-Partisans @cpartisans · 22h
At the command of the terrorist Lukashenka, #Belarusian Railway allows the occupying troops to enter our land. We encrypted some of BR's servers, databases and workstations to disrupt its operations. ❗ Automation and security systems were NOT affected to avoid emergency situations

9:21 AM · Jan 24, 2022 · TweetDeck

366 Retweets 171 Quote Tweets 788 Likes

In public media reports, it has been stated that the rail service's website issued a warning to passengers that some e-ticket systems were unavailable (source: rw[.]by), seemingly confirming the Cyber-Partisans' claims that they targeted network assets in order to disrupt operations. The Belarusian government has not commented on the incident.

On Tuesday 24 January, Curated Intelligence member @SttyK obtained documents from Cyber-Partisans, which the group claimed would help SttyK "understand some of the methods used" during the attack. Initially SttyK reached out to the group seeking access to the malware used in the attack, which would have then been studied. However, the group declined to share the code, but noted they would "gladly do that once the authoritarian regime in Belarus is gone."

Known Information:

Based on public reporting and previous interviews, the Belarusian Cyber-Partisans are "a group of 15 self taught hacktivists who claim to have assistance and support from disaffected Belarusian security forces" (source: CyberScoop). The group has been closely associated with a series of government website defacement operations. Last August, the group spoke to Patrick Howell O'Neill at Technology Review, in a rather informative interview, should anyone want some additional background.

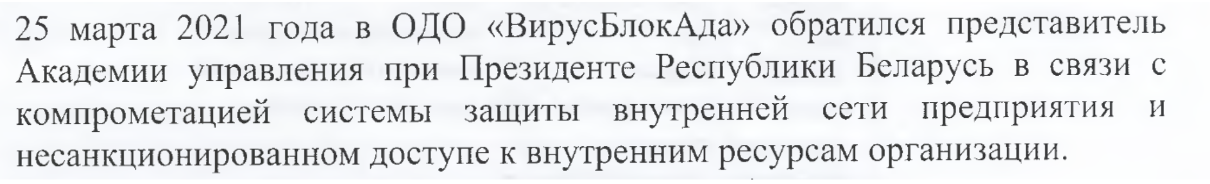
New Information:

As mentioned, SttyK reached out to the group in order to obtain malware samples for study. Instead, what the group responded with were a series of documents. These documents represent a report based on an investigation into an attack on 14 March 2021, which concluded on 8 April of the same year.

Editor Note: *One of the first questions asked internally by Curated Intelligence members was "why?". Why are they sharing such details, and what do they have to gain by exposing a previously released incident report? There are a number of answers to that question, but the key answer is exposure. As is the case with articles in major publications, blogs such as this one give hacktivists attention to their cause. So then the question becomes, is the information they shared with us of importance to the public (yes, it is). Thus giving them attention is worth the trade-off in our opinions, and serves our goal of informing the public.*

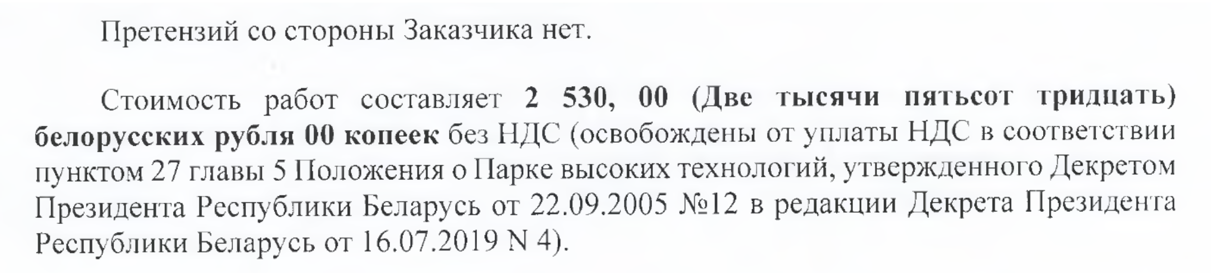
The Stolen Incident Response Report:

- The report was first mentioned in a YouTube video on the Cyber-Partisans' own YouTube Channel in November 2021 (see here)
- The investigation and report began on 25 March 2021 and was done by VirusBlokAda (the antivirus firm that also first discovered Stuxnet)
- The incident report costed 2530.00 BYN (worth an estimated $1,000 USD)
- In the report, the initial date of compromise was discovered to be 14 March 2021
- According to the report, the victim was the Academy of Public Administration under the President of the Republic of Belarus



25 марта 2021 года в ОДО «ВирусБлокАда» обратился представитель Академии управления при Президенте Республики Беларусь в связи с компрометацией системы защиты внутренней сети предприятия и несанкционированном доступе к внутренним ресурсам организации.

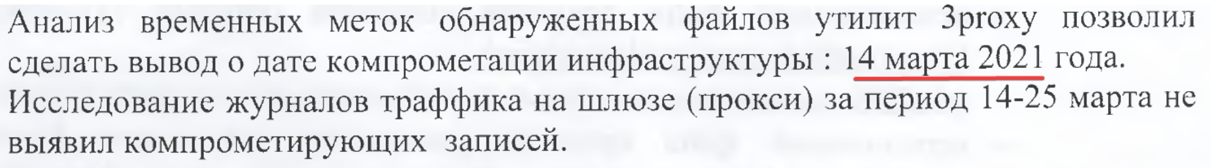
Fig. 1 - Confirmation of who the victim was in the report



Претензий со стороны Заказчика нет.

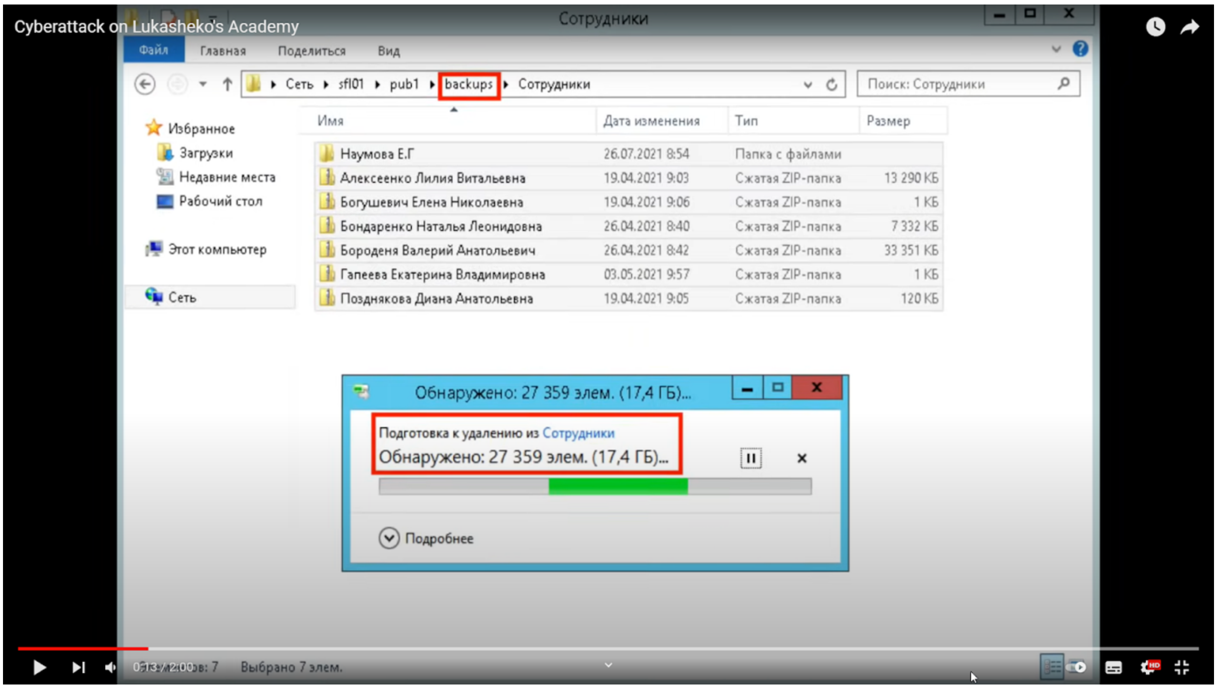
Стоимость работ составляет **2 530, 00 (Две тысячи пятьсот тридцать) белорусских рубля 00 копеек** без НДС (освобождены от уплаты НДС в соответствии пунктом 27 главы 5 Положения о Парке высоких технологий, утвержденного Декретом Президента Республики Беларусь от 22.09.2005 №12 в редакции Декрета Президента Республики Беларусь от 16.07.2019 N 4).

Fig. 2 - The incident report costed 2530.00 BYN (worth $1,000)



Анализ временных меток обнаруженных файлов утилит 3proxy позволил сделать вывод о дате компрометации инфраструктуры : 14 марта 2021 года. Исследование журналов траффика на шлюзе (прокси) за период 14-25 марта не выявил компрометирующих записей.

Fig. 3 - Initial date of compromise was 14 March 2021



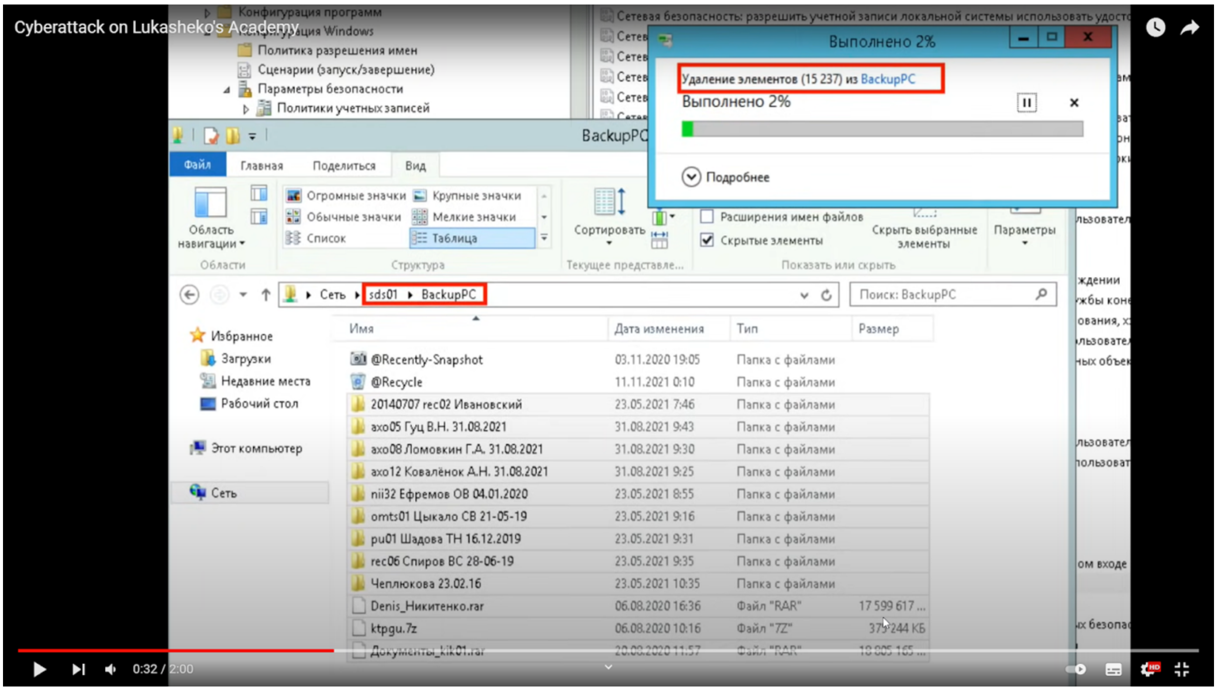
Имя	Дата изменения	Тип	Размер
Наумова Е.Г	26.07.2021 8:54	Папка с файлами	
Алексеенко Лилия Витальевна	19.04.2021 9:03	Сжатая ZIP-папка	13 290 КБ
Богушевич Елена Николаевна	19.04.2021 9:06	Сжатая ZIP-папка	1 КБ
Бондаренко Наталья Леонидовна	26.04.2021 8:40	Сжатая ZIP-папка	7 332 КБ
Бороденя Валерий Анатольевич	26.04.2021 8:42	Сжатая ZIP-папка	33 351 КБ
Гапеева Екатерина Владимировна	03.05.2021 9:57	Сжатая ZIP-папка	1 КБ
Позднякова Диана Анатольевна	19.04.2021 9:05	Сжатая ZIP-папка	120 КБ

Обнаружено: 27 359 элем. (17,4 ГБ)...

Подготовка к удалению из Сотрудники

Обнаружено: 27 359 элем. (17,4 ГБ)...

Fig. 4 - Screenshot of files containing employee data being deleted



Выполнено 2%

Удаление элементов (15 237) из BackupPC

Выполнено 2%

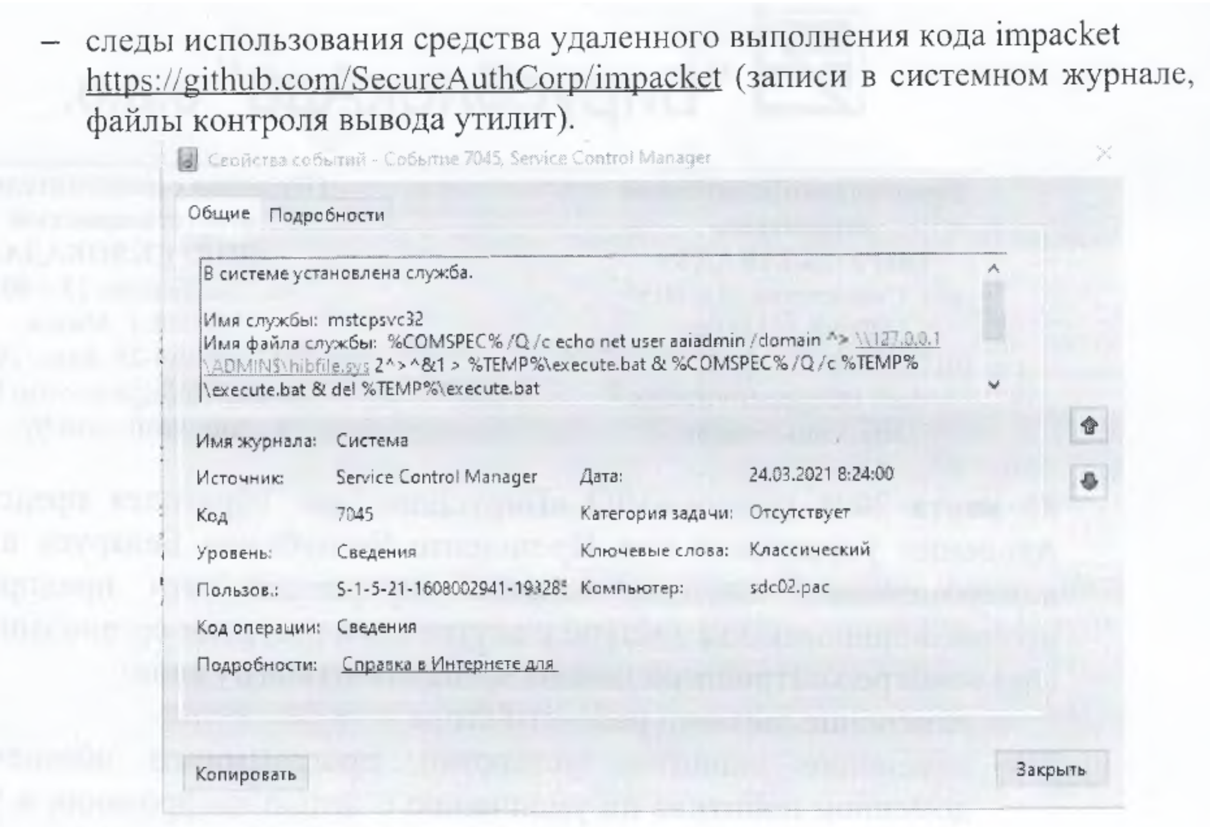
Подробнее

Сеть ▸ sds01 ▸ BackupPC

Поиск: BackupPC

Имя	Дата изменения	Тип	Размер
@Recently-Snapshot	03.11.2020 19:05	Папка с файлами	
@Recycle	11.11.2021 0:10	Папка с файлами	
20140707 rec02 Ивановский	23.05.2021 7:46	Папка с файлами	
axo05 Гуц В.Н. 31.08.2021	31.08.2021 9:43	Папка с файлами	
axo08 Ломовкин Г.А. 31.08.2021	31.08.2021 9:30	Папка с файлами	
axo12 Ковалёнок А.Н. 31.08.2021	31.08.2021 9:25	Папка с файлами	
nii32 Ефремов ОВ 04.01.2020	23.05.2021 8:55	Папка с файлами	
omts01 Цыкало СВ 21-05-19	23.05.2021 9:16	Папка с файлами	
pu01 Шадова ТН 16.12.2019	23.05.2021 9:31	Папка с файлами	
rec06 Спиров ВС 28-06-19	23.05.2021 9:35	Папка с файлами	
Чеплюкова 23.02.16	23.05.2021 10:35	Папка с файлами	
Denis_Никитенко.rar	06.08.2020 16:36	Файл "RAR"	17 599 617 ...
ktpgu.7z	06.08.2020 10:16	Файл "7Z"	379 244 КБ
Документы_kik01.rar	20.08.2020 11:57	Файл "RAR"	18 805 165 ...

Fig. 5 - Screenshot of files in the backup server being deleted



– следы использования средства удаленного выполнения кода impacket https://github.com/SecureAuthCorp/impacket (записи в системном журнале, файлы контроля вывода утилит).

Свойства событий - Событие 7045, Service Control Manager

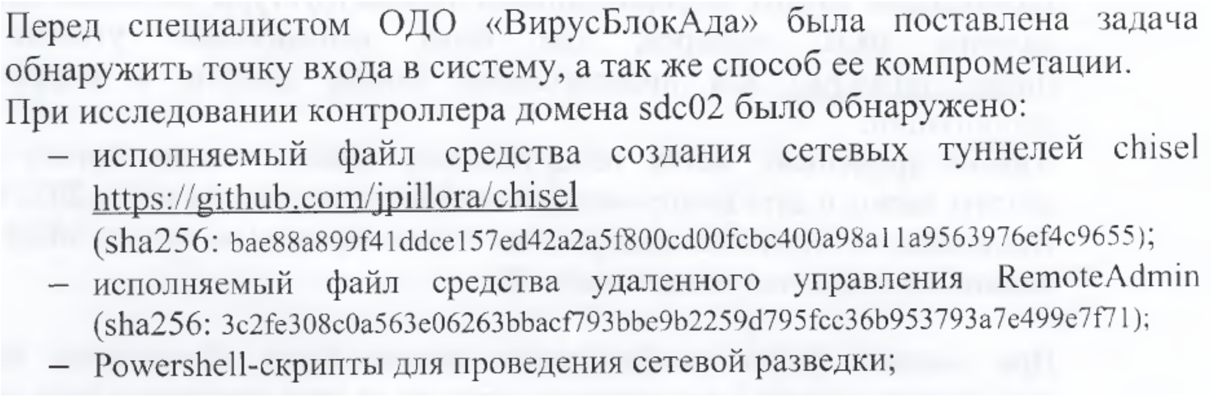
```
В системе установлена служба.

Имя службы:  mstcpsvc32
Имя файла службы:  %COMSPEC% /Q /c echo net user aaiadmin /domain ^> \\127.0.0.1
\ADMIN$\hibfile.sys 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%
\execute.bat & del %TEMP%\execute.bat
```

Имя журнала:	Система		
Источник:	Service Control Manager	Дата:	24.03.2021 8:24:00
Код	7045	Категория задачи:	Отсутствует
Уровень:	Сведения	Ключевые слова:	Классический
Пользов.:	S-1-5-21-1608002941-193285	Компьютер:	sdc02.pac
Код операции:	Сведения		
Подробности:	Справка в Интернете для		

Fig. 6 - Screenshot of the report mentioning the use of Impacket

Impacket - https://github.com/SecureAuthCorp/impacket



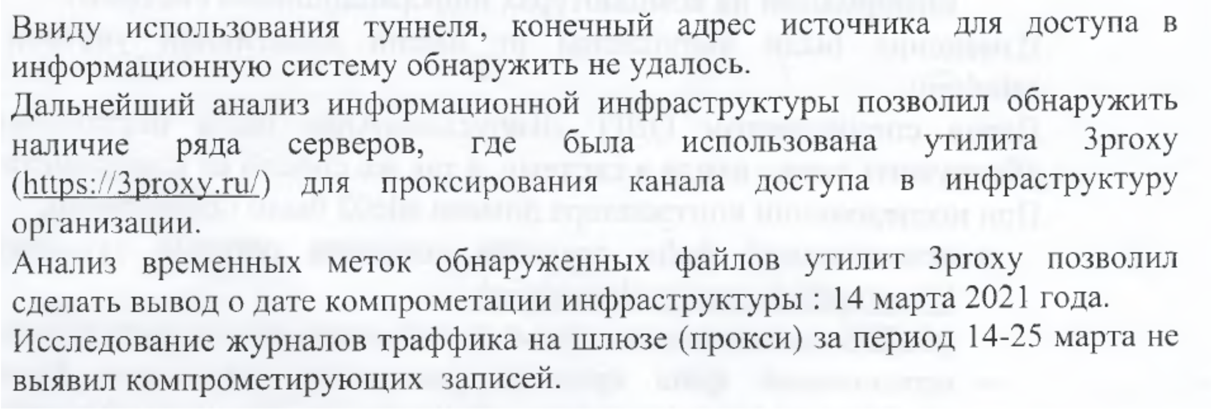
Перед специалистом ОДО «ВирусБлокАда» была поставлена задача обнаружить точку входа в систему, а так же способ ее компрометации.

При исследовании контроллера домена sdc02 было обнаружено:

- исполняемый файл средства создания сетевых туннелей chisel https://github.com/jpillora/chisel (sha256: bae88a899f41ddce157ed42a2a5f800cd00fcbc400a98a11a9563976ef4c9655);
- исполняемый файл средства удаленного управления RemoteAdmin (sha256: 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71);
- Powershell-скрипты для проведения сетевой разведки;

Fig. 7 - Screenshot of the report mentioning the use of Chisel

Chisel - https://github.com/jpillora/chisel



Ввиду использования туннеля, конечный адрес источника для доступа в информационную систему обнаружить не удалось.

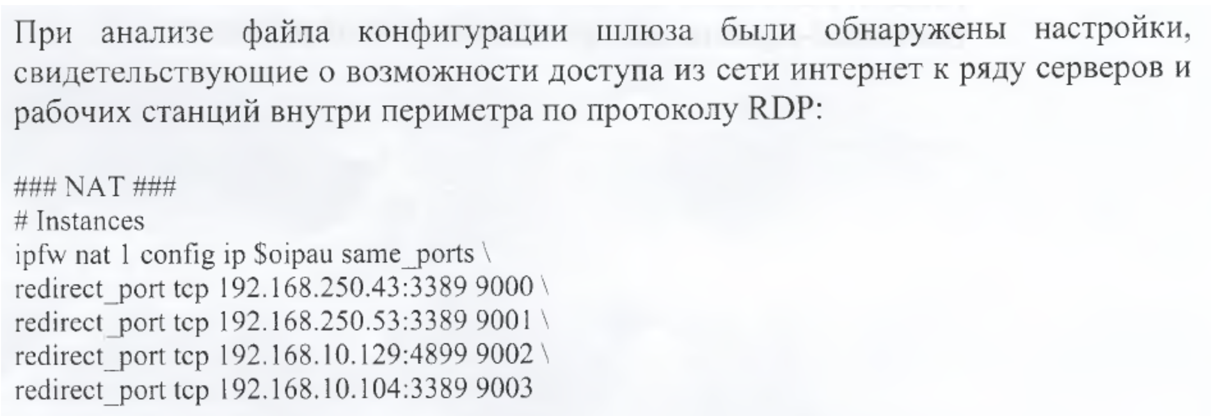
Дальнейший анализ информационной инфраструктуры позволил обнаружить наличие ряда серверов, где была использована утилита 3proxy (https://3proxy.ru/) для проксирования канала доступа в инфраструктуру организации.

Анализ временных меток обнаруженных файлов утилит 3proxy позволил сделать вывод о дате компрометации инфраструктуры : 14 марта 2021 года.

Исследование журналов траффика на шлюзе (прокси) за период 14-25 марта не выявил компрометирующих записей.

Fig. 8 - Screenshot of the report mentioning the use of 3proxy[.]ru

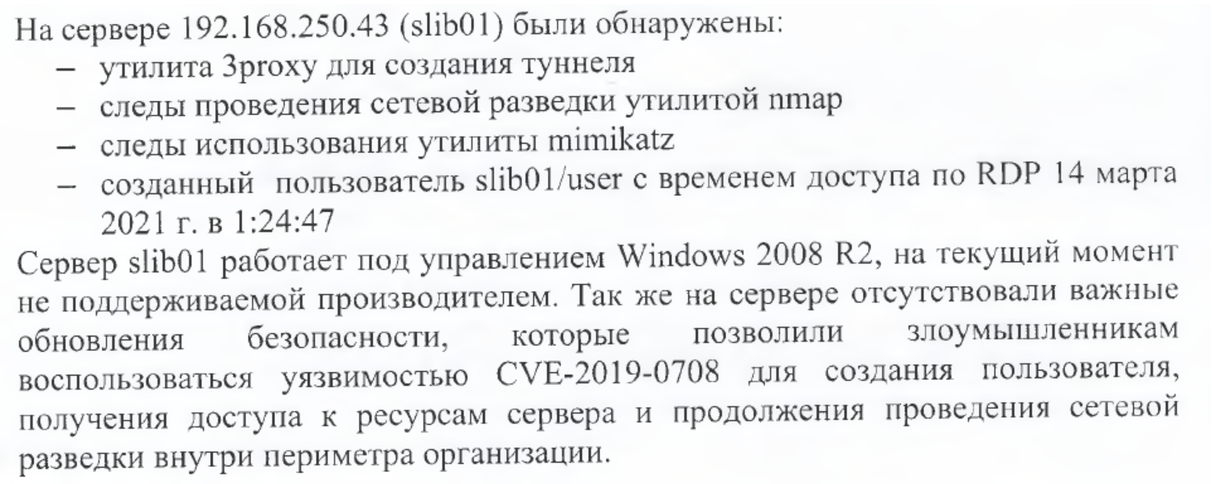
3proxy - https://3proxy.org/



При анализе файла конфигурации шлюза были обнаружены настройки, свидетельствующие о возможности доступа из сети интернет к ряду серверов и рабочих станций внутри периметра по протоколу RDP:

```
### NAT ###
# Instances
ipfw nat 1 config ip $oipau same_ports \
redirect_port tcp 192.168.250.43:3389 9000 \
redirect_port tcp 192.168.250.53:3389 9001 \
redirect_port tcp 192.168.10.129:4899 9002 \
redirect_port tcp 192.168.10.104:3389 9003
```

Fig. 9 - Screenshot of the report mentioning 3389 (RDP) port forwarding over TCP



На сервере 192.168.250.43 (slib01) были обнаружены:

- утилита 3proxy для создания туннеля
- следы проведения сетевой разведки утилитой nmap
- следы использования утилиты mimikatz
- созданный пользователь slib01/user с временем доступа по RDP 14 марта 2021 г. в 1:24:47

Сервер slib01 работает под управлением Windows 2008 R2, на текущий момент не поддерживаемой производителем. Так же на сервере отсутствовали важные обновления безопасности, которые позволили злоумышленникам воспользоваться уязвимостью CVE-2019-0708 для создания пользователя, получения доступа к ресурсам сервера и продолжения проведения сетевой разведки внутри периметра организации.

Fig. 10 - Screenshot of the report mentioning the use of Nmap, Mimikatz, CVE-2019-0708

Considering this was a full incident response investigation that cost less than $1,000 it is unsurprising that the findings are unclear. The attack chain was not fully explained, but we **have tried to piece it together** as best we can with the help of a Curated Intelligence member, @0xDISREL, who can read and write Russian. We still are not confident this is a full accurate representation of the group's TTPs, but should help nonetheless.

Summary of Attack:

- Initial access via BlueKeep RCE (CVE-2019-0708) in RDP in a Windows Server 2008 R2 system
- Used the 3proxy[.]ru service to launch attacks from a VPS
- Use of Mimikatz to dump LSASS (SYSTEM level privileges are required however, how they obtained these is currently unclear)
- Nmap to identify systems (used Nmap to identify systems with Port 3389 open)
- Used RDP to move laterally
- Eventually landed on the victim's Domain Controller
- Configured TCP port forwarding to open Port 3389 to the internet for persistent access
- Deleted data (such as employee records) from live and backup systems

Indicators of Compromise (IOCs):

Type	Indicator	Context
SHA256	3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71	RemoteAdmin.exe
SHA256	bae88a899f41ddce157ed42a2a5f800cd00fcbc400a98a11a9563976ef4c9655	psexec.py
Domain	3proxy[.]ru	VPS Proxy

Threat Hunting Tips:

Executed commands:

- mstcpsvc32 %COMSPEC% /Q /c echo net user aaiadmin /domain ^> \\127.0.0.1\ADMIN$\hibfile.sys 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat

Forwarded Ports:

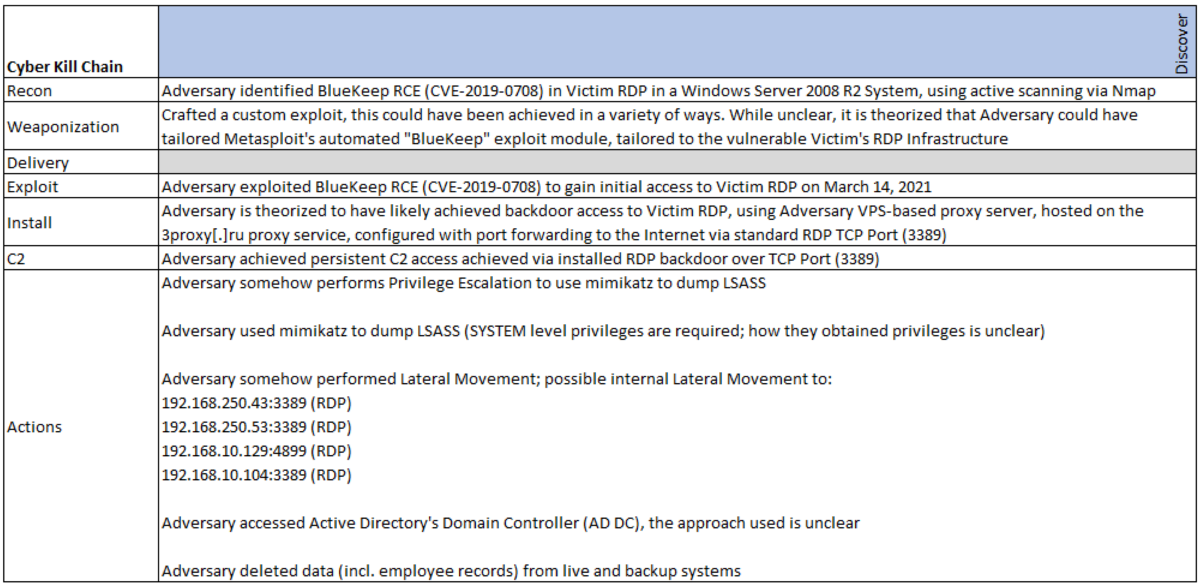
- 3389 (RDP) -> Port 9000
- 3389 (RDP) -> Port 9001
- 4899 (RAdmin) -> Port 9002
- 3389 (RDP) -> Port 9003

User Accounts:

- They used the default user **aaiadmin**

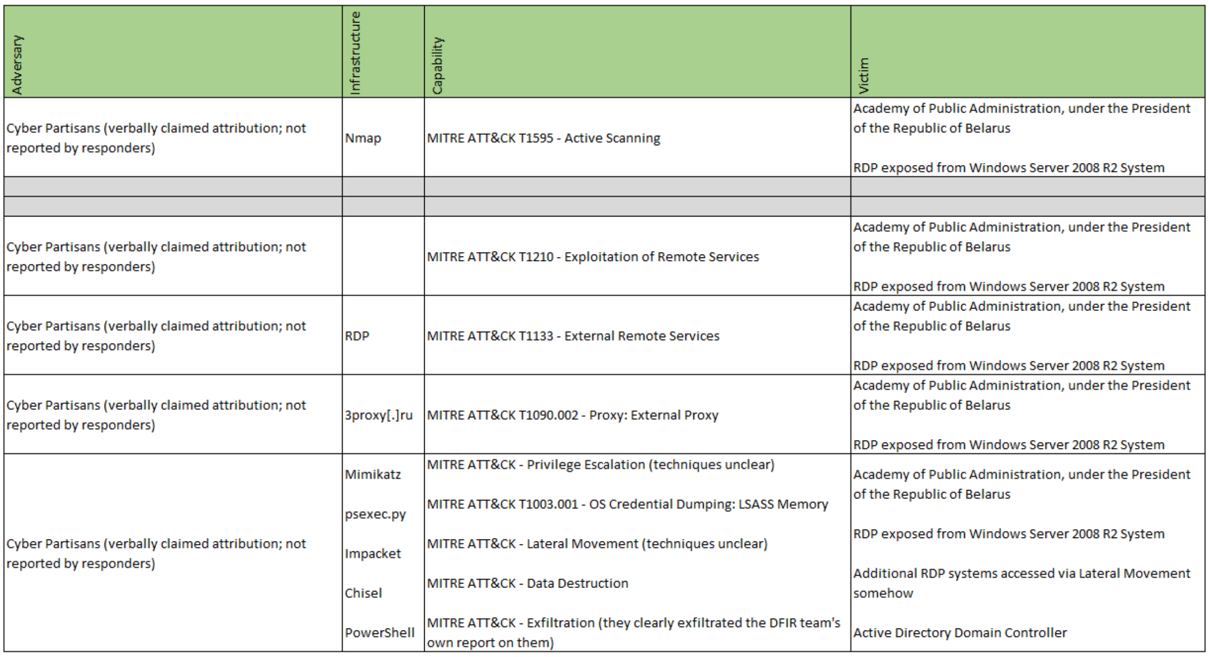
Cyber Kill Chain:

Curated Intelligence member, @TrevorGiffen, roughly mapped the intrusion analysis to Cyber Kill Chain, Diamond Model, and MITRE ATT&CK.



Cyber Kill Chain	Discover
Recon	Adversary identified BlueKeep RCE (CVE-2019-0708) in Victim RDP in a Windows Server 2008 R2 System, using active scanning via Nmap
Weaponization	Crafted a custom exploit, this could have been achieved in a variety of ways. While unclear, it is theorized that Adversary could have tailored Metasploit's automated "BlueKeep" exploit module, tailored to the vulnerable Victim's RDP Infrastructure
Delivery	
Exploit	Adversary exploited BlueKeep RCE (CVE-2019-0708) to gain initial access to Victim RDP on March 14, 2021
Install	Adversary is theorized to have likely achieved backdoor access to Victim RDP, using Adversary VPS-based proxy server, hosted on the 3proxy[.]ru proxy service, configured with port forwarding to the Internet via standard RDP TCP Port (3389)
C2	Adversary achieved persistent C2 access achieved via installed RDP backdoor over TCP Port (3389)
Actions	Adversary somehow performs Privilege Escalation to use mimikatz to dump LSASS Adversary used mimikatz to dump LSASS (SYSTEM level privileges are required; how they obtained privileges is unclear) Adversary somehow performed Lateral Movement; possible internal Lateral Movement to: 192.168.250.43:3389 (RDP) 192.168.250.53:3389 (RDP) 192.168.10.129:4899 (RDP) 192.168.10.104:3389 (RDP) Adversary accessed Active Directory's Domain Controller (AD DC), the approach used is unclear Adversary deleted data (incl. employee records) from live and backup systems

Diamond Model with MITRE ATT&CK:



Adversary	Infrastructure	Capability	Victim
Cyber Partisans (verbally claimed attribution; not reported by responders)	Nmap	MITRE ATT&CK T1595 - Active Scanning	Academy of Public Administration, under the President of the Republic of Belarus RDP exposed from Windows Server 2008 R2 System
Cyber Partisans (verbally claimed attribution; not reported by responders)		MITRE ATT&CK T1210 - Exploitation of Remote Services	Academy of Public Administration, under the President of the Republic of Belarus RDP exposed from Windows Server 2008 R2 System
Cyber Partisans (verbally claimed attribution; not reported by responders)	RDP	MITRE ATT&CK T1133 - External Remote Services	Academy of Public Administration, under the President of the Republic of Belarus RDP exposed from Windows Server 2008 R2 System
Cyber Partisans (verbally claimed attribution; not reported by responders)	3proxy[.]ru	MITRE ATT&CK T1090.002 - Proxy: External Proxy	Academy of Public Administration, under the President of the Republic of Belarus RDP exposed from Windows Server 2008 R2 System
Cyber Partisans (verbally claimed attribution; not reported by responders)	Mimikatz psexec.py Impacket Chisel PowerShell	MITRE ATT&CK - Privilege Escalation (techniques unclear) MITRE ATT&CK T1003.001 - OS Credential Dumping: LSASS Memory MITRE ATT&CK - Lateral Movement (techniques unclear) MITRE ATT&CK - Data Destruction MITRE ATT&CK - Exfiltration (they clearly exfiltrated the DFIR team's own report on them)	Academy of Public Administration, under the President of the Republic of Belarus RDP exposed from Windows Server 2008 R2 System Additional RDP systems accessed via Lateral Movement somehow Active Directory Domain Controller