

# Hacktivist group shares details related to Belarusian Railways hack

---

[curatedintel.org/2022/01/hacktivist-group-shares-details-related.html](https://curatedintel.org/2022/01/hacktivist-group-shares-details-related.html)

BushidoToken

*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.



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 hackers 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 hackers 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 Зроху позволил сделать вывод о дате компрометации инфраструктуры : 14 марта 2021 года. Исследование журналов трафика на шлюзе (прокси) за период 14-25 марта не выявил компрометирующих записей.

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

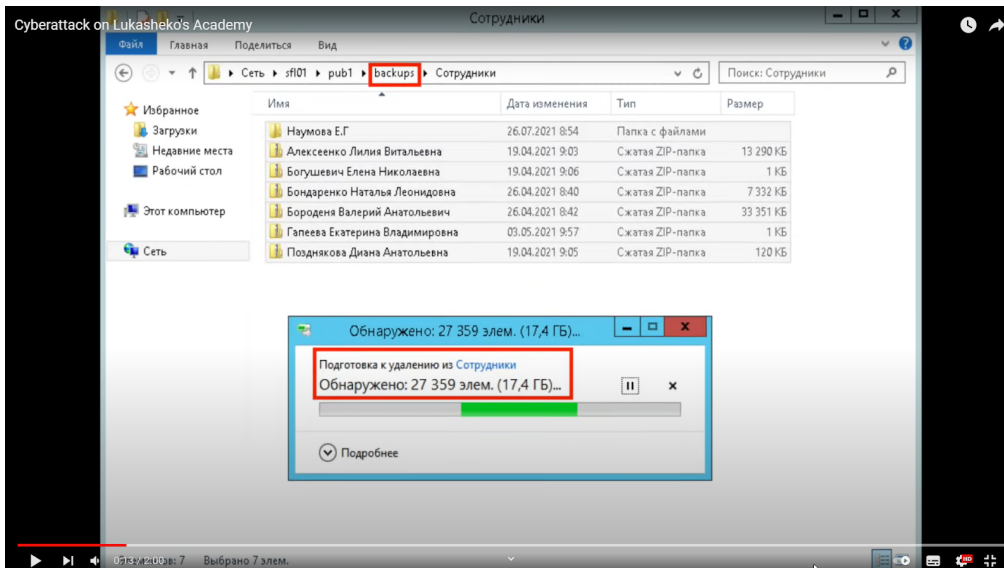


Fig. 4 - Screenshot of files containing employee data being deleted

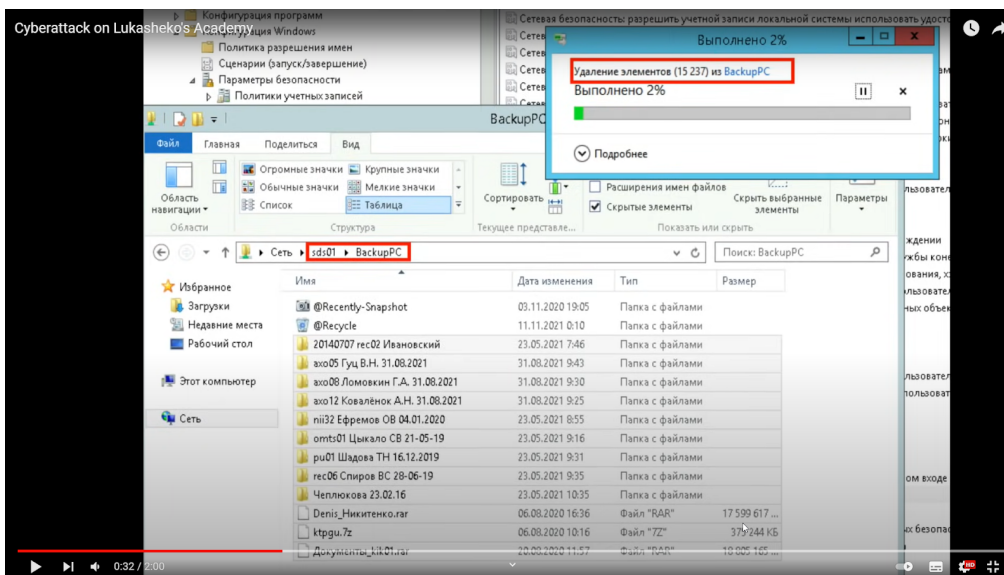


Fig. 5 - Screenshot of files in the backup server being deleted

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

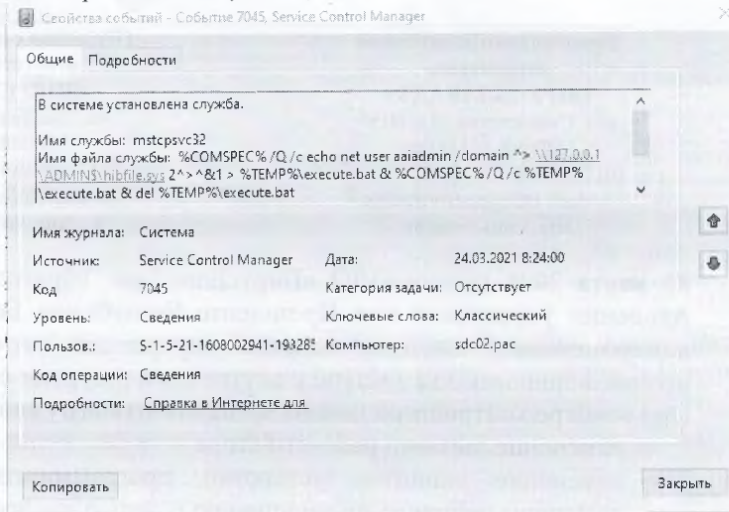


Fig. 6 - Screenshot of the report mentioning the use of Impacket  
Impacket - <https://github.com/SecureAuthCorp/impacket>

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 трафика 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 3проху 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:**

```
mstcpssc32 %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.