

---

# An Incredibly Organized Ransomware

- CONTI -

# \$whoami

Ömer Faruk Çulha

PurpleBox -> Cyber Security Engineer

Sakarya Üniversitesi -> Makine Müh.

<https://twitter.com/0x1337root>

<https://tryhackme.com/p/0x1337root>

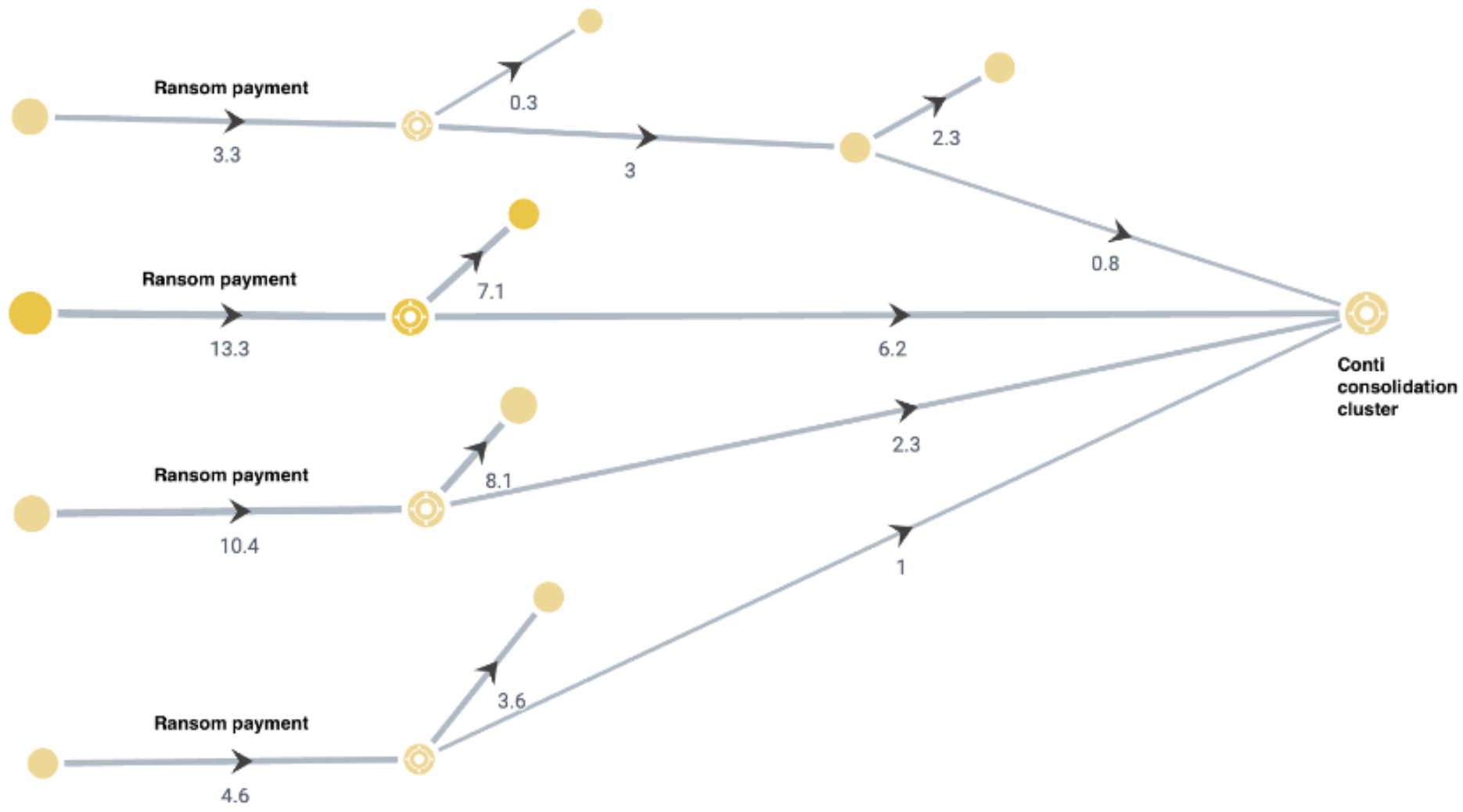
<https://www.linkedin.com/in/ömer-faruk-çulha-b95880195>



# Ransomware Nedir ?

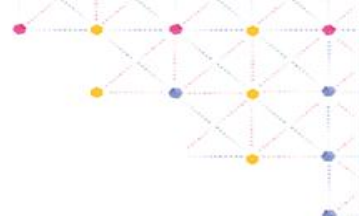






# CONTI ?





BANNED

m1Geelka  
RWD mass

✖ Заблокировано

Регистрация: 29.04.2020  
Сообщений: 52  
Пользователь: 77

05.08.2021

← □ #1

⊗ Пожалуйста, обратите внимание, что пользователь заблокирован

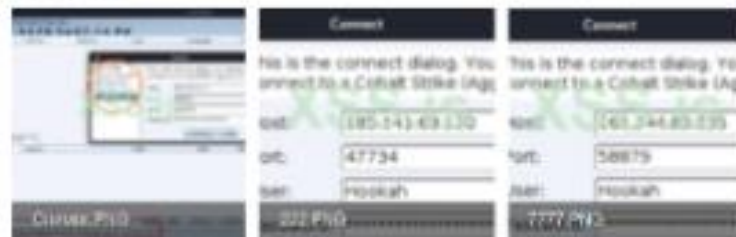
Тупой развод а не работа. Пенестерол они набирают, да конечно... Собирают ребят для обработки сетей Active Directory. Ловар юзают - Conti. Снимаю там их ip адрес серверов нобольга и типа материалы обучения. 1500\$ да конечно набирают ловар и делят между собой деньги, а пиданов корки! тем что дадут знать когда жертва заплатит. Админ в чате был - Tokyo, его жаба - cicada3301@strong.pw. Знайте пидораса в лицо! Куда нужно я уже отправил данные поэтому пусть моют данные сервера и все остальное. А для ребят собираю все материалы по обучению -)

All good

Их чат в Telegram - bk7aan42fmm4nxbse4dpxu7njz4e2hqvtkbhyfiov7yq2bjabed.onion

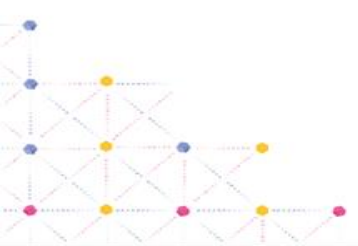
Тот кто набирает на типа работу Пенестерол 🤔🤔🤔🤔 - <https://www.leasemembers.com/members/229126/> его жаба - i\_jack\_siorci@strong.jp

Вложения



С Жаба

👍 Like + Цитата 🗨 Ответ






kilobyte



Group: Пользователь  
 Posts: 38  
 Joined: 11/29/2016  
 Пользователь №: 74 394  
 Activities: [activity](#)

Reputation:   
 (1% - хорошо)

08/22/2017, 17:33

## Hermes 2.1 Ransomware The

software did not work and will not work on RU, UA, BY.

- \* Work offline, communication via email.
- \* Written in C.
- \* Weight 45-55kb (each build is unique).
- \* Work on x86 / x64, servers: 2003 and higher, XP, 7,8,10.
- \* Easy to crumble.
- \* Encryption AES256 + RSA2048, a unique key for each system, and each file.
- \* Only the owner of a private RSA key can decrypt the files, BleepingComputer agrees with this.
- \* \_\_ <https://www.bleepingcomputer.com/forums/t/640086/hermes-ransom-help-support-topic-decrypt-informationhtml-ransom-note/>
- \* Restore work after reboot if the encryption was not completed.
- \* Drop user-key and instructions in each folder.
- \* 809 file extensions, detailed information in the archive.
- \* Encrypt files of any size.
- \* Data is written on top of the current file, which greatly complicates data recovery with the help of R-studio, Recuva, etc.
- \* Request for privilege elevation from the user, delete shadow copies and backups
- \* Price of the set: \$ 300
- \* Rebid price for email addresses: \$ 50
- \* Included: a build with 2 your email addresses, a decoder builder, a unique pair of RSA keys.

PS: the implementation / change of almost any functional, on a separate financial component, is discussed.

There are no Manibekovs.

We reserve the right to refuse sale without explanation.

AB scan at the moment: \_\_ <https://viruscheckmate.com/id/NuASrGO3je1V>

- \* Software does not work in RU, UA, BY countries.
- \* work offline, communication by e-mail.
- \* Write on C
- \* Build size 45-55kb.
- \* Work on x86 / x64, servers: 2003 and higher, XP, 7,8,10.





## Пентестер? Тогда к нам!

By IT\_Work, June 23 in [Job] - search, execution of work

Follow 4

Start new topic

Reply to this topic

IT\_Work

megabyte



Real registration

19

57 posts

Joined

05/21/21 (ID: 136714)

Activity

Другие / other

Posted June 23

Report post

Ищем и набираем в команду пентестеров!

### Требования:

- Понимание структуры Active Directory сайт администрировании Windows
- Понимание основ маршрутизации Nat, рmku, socks, http, https, ssh
- Понимание работы сетевых протоколов
- Знание любого из языков программирования
- Знание pentest (тестирование на безопасность) большой плюс

### Условия:

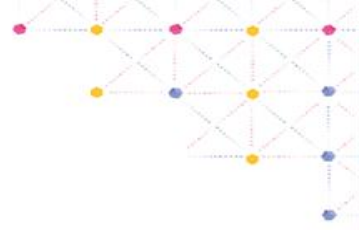
- Мы предлагаем Вам своевременную зарплату в размере от 1500\$ (выплаты по курсу на день оплаты в btc)
- Работа полностью УДАЛЕННАЯ, 5 дней в неделю, СБ и ВС выходные.
- График работы с 15-00 до 01-00
- Оплачиваемый отпуск
- У нас в условиях есть постоянный рост - на каждый успех вы получаете постоянную прибавку плюс мгновенный бонус

Если Вас заинтересовала эта вакансия, вышлите свое резюме в пм - если ваша кандидатура нас заинтересует - мы вышлем оплачиваемое (20k.r.в btc по курсу) тестовое задание.

The image shows the Cobalt Strike application interface. At the top, there is a menu bar with 'Cobalt Strike', 'View', 'Attacks', 'Reporting', and 'Help'. Below the menu is a toolbar with various icons. A secondary menu bar contains tabs for 'external', 'internal', 'listener', 'user', 'computer', 'note', and 'pr'. The main area is currently empty. A 'Connect' dialog box is open in the center, containing a list of IP addresses: 'New Profile', '162.244.80.235', '85.93.88.165', '185.141.63.120', and '82.118.21.1'. The '82.118.21.1' entry is highlighted. To the right of the list, there is a text box with the instruction: 'This is the connect dialog. You should use it to connect to a Cobalt Strike (Aggressor) team server.' Below this are input fields for 'Host:' (82.118.21.1), 'Port:' (56161), 'User:' (Hookah), and 'Password:' (masked with asterisks). 'Connect' and 'Help' buttons are at the bottom of the dialog. Below the dialog, there are tabs for 'Event Log X' and 'Listeners X'. The 'Listeners X' tab is active, showing a table with columns: 'name', 'payload', 'host', 'port', 'bindto', and 'beacons'. The table is currently empty. At the bottom of the interface, there are buttons for 'Add', 'Edit', 'Remove', 'Restart', and 'Help'. A red box highlights the 'Add' button and the text 'Hookah@82.118.21.1 Hookah@185.141.63.120 Hookah@162.244.80.235' below it.

name	payload	host	port	bindto	beacons
------	---------	------	------	--------	---------

Hookah@82.118.21.1 Hookah@185.141.63.120 Hookah@162.244.80.235



```
'++07. Metasploit+'
'0. Network Pentesting+'
'10. Управление доступом Повышение привилегий доступа'
'11. Управление доступом Установка бэкдора'
'12. Управление доступом Взлом паролей'
'13. Управление доступом Удаление следов своей деятельности'
'14. Дополнительные лекции'
'15. Визуализация атак с помощью Armitage'
'1.Powershell for Pentesters+'
'1. Windows Red Team Lab+'
'1. Введение'
'1. Кряк 2019'
'2. Attacking and Defending Active Directory+'
'2. Реверс и эксплойтов'
'2. Установка лабораторного окружения'
'34. WMI Attacks and Defense +'
'3. Введение в Metasploit'
'4. Предварительный сбор информации об атакуемом объекте'
'5. Сканирование объекта'
'6. Получение доступа к системе через серверные атаки'
'7. Получение доступа к системе через клиентские атаки'
'8. Способы создания троянской программы'
'9. Управление доступом Взаимодействие со взломанным компьютером'
  Abusing-SQL-Server-Trusts.pdf
' Cobalt Strike'
  GCB
  SQLServe.txt
'Windows Red Team Lab.docx'
'Злоупотребление доверием к SQL Server в домене Windows.docx'
'Новый текстовый документ.txt'
  Реверс-инжиниринг
```

- Compiler-based obfuscation teknikleri kullanarak güvenlik ürünlerinden kaçınmaya giriş.
- rclone ile kurban verisini MEGA güvenli bulut depolamaya çekmek.
- Ngrok güvenli tünel kullanılarak hacklenmiş ağa nasıl RDP ile bağlanılır?
- SMB brute-force saldırıları gerçekleştirme kılavuzu.
- İşletim sistemi ve Tor üzerinden internet trafiğini anonimleştirme hakkında bir eğitim.
- Hedef ağ içerisinde privilege escalation ve admin yetkileri edinme eğitimi.

```
'++07. Metasploit+'  
'0. Network Pentesting+'  
'10. Управление доступом Повышение привилегий доступа'  
'11. Управление доступом Установка бэкдора'  
'12. Управление доступом Взлом паролей'  
'13. Управление доступом Удаление следов своей деятельности'  
'14. Дополнительные лекции'  
'15. Визуализация атак с помощью Armitage'  
'1. Powershell for Pentesters+'  
'1. Windows Red Team Lab+'  
'1. Введение'  
'1. Кряк 2019'  
'2. Attacking and Defending Active Directory+'  
'2. Реверс и эксплойтов'  
'2. Установка лабораторного окружения'  
'34. WMI Attacks and Defense +'
```

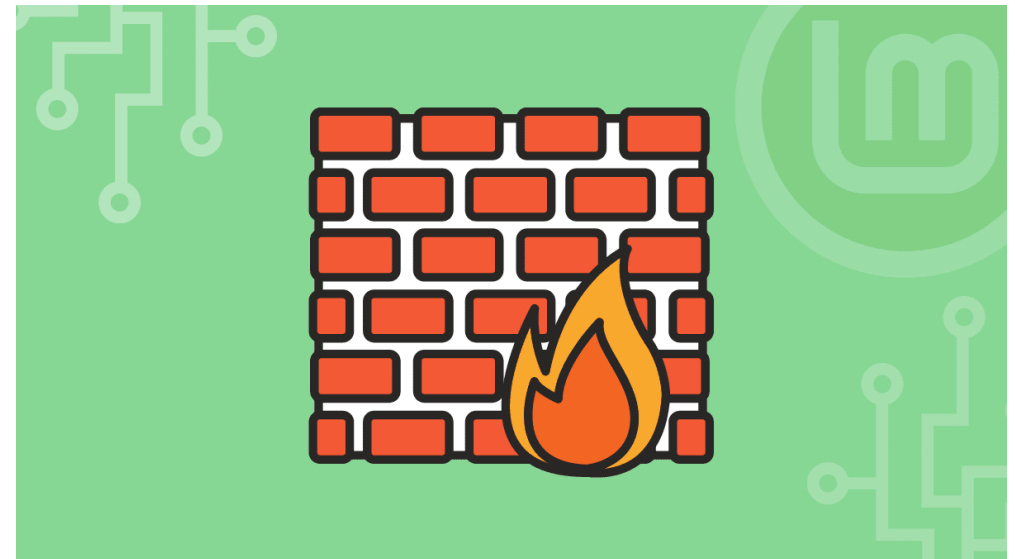
```
'3. Введение в Metasploit'  
'4. Предварительный сбор информации об атакуемом объекте'  
'5. Сканирование объекта'  
'6. Получение доступа к системе через серверные атаки'  
'7. Получение доступа к системе через клиентские атаки'  
'8. Способы создания троянской программы'  
'9. Управление доступом Взаимодействие со взломанным компьютером'  
'Abusing-SQL-Server-Trusts.pdf'  
'Cobalt Strike'  
'GCB'  
'SQLServe.txt'  
'Windows Red Team Lab.docx'  
'Злоупотребление доверием к SQL Server в домене Windows.docx'  
'Новый текстовый документ.txt'  
'Реверс-инжиниринг'
```

# Teknik ?

- PrintNightmare (CVE-2021-1675)
  - CVE-2021-1675
  - CVE-2021-34527
  - CVE-2021-36958



- Fortigate Firewall RCE
  - CVE-2018-13379
  - CVE-2018-13374



# İlk Temas ?

- Phishing
- Geniş zaafiyet taramaları
- Zararlı siteler
- Sahte telefon çağrıları
- Brute-Force
- Distribütör malware

Sign in to use your favorite productivity apps from any device



Microsoft  
Office 365



**You Have Received (2) Pdf online**

Message ID "5467454678948-546"

Reference: MLK355344343434-S5894 22/02/2021

This E-mail was sent from Scanner "RNP583879051AFA"

[CLICK HERE TO VIEW DOCUMENT>>>](#)

Adobe PDF-Microsoft Online 2021



Microsoft | Office Products ▾ Resources ▾ Templates Support My account [Buy now](#)

# Aşama - Recon

- Domain-Controller
- Backup Sunucuları
- Yanal hareketler
- Kritik veriler



# Aşama - Sızıntı

- rclone
- MEGA
- ChaCha8





# Aşama - Pazarlık

```
readme.txt - Notepad
File Edit Format View Help
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :|
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION :
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us as soon as possible.

---BEGIN ID---
[REDACTED]
---END ID---
```

```
RyukReadMe.txt - Notepad
File Edit Format View Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
WayneEvenson@protonmail.com
or
WayneEvenson@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk

No system is safe
```



# CONTI Recovery service

If you are looking at this page right now, that means that your network was successfully breached by CONTI team.

All of your files, databases, application files etc were encrypted with military-grade algorithms.

If you are looking for a free decryption tool right now - there's none.

Antivirus labs, researches, security solution providers, law agencies won't help you to decrypt the data.

If you are interested in our assistance upon this matter - you should upload README.TXT file to be provided with further instructions upon decryption.

No file selected.

[Web mirror](#)

[Tor mirror](#)

## CONTI Recovery service



Hello, are you ready to negotiate?

6 days ago

As you already know - your network and all of your data were encrypted by CONTI team. Besides the encryption process we've downloaded a large pack of your internal documents and files that will be published in case our negotiations fail. How it happens can be seen on our website  
The recovery price is \$100.000. If you want to make sure we can recover all of your data - you can send us the two files of your choice and we will decrypt them free of charge.  
If we reach mutual agreement your will be provided with decryption tool, none of your internal data will be published and you will be provided with security tips on how to avoid further breaches.  
We strongly recommend to review our offer in a timely manner.

6 days ago



Hi are you there?? Kindly help us please

5 days ago



yes

5 days ago



Kindly help us we are ready to pay you

5 days ago

Price is very high? can you provide some discount to us?

5 days ago

How much time will it takes to decrypt after sending money to you

5 days ago



We will give the decrypt app immediately after payment and you can decipher everything for an hour

5 days ago

In addition, we stole your 50 gigabyte data  
Within 24 hours, we will download the list of what downloaded from your network

5 days ago



tell us where we have to pay and kindly provide some discount please

5 days ago



Do you wait for listing or want to pay fast?

5 days ago

[full-listing\\_legacy.txt \[4MB\]](#)

5 days ago



Payment confirmed. Soon we'll send you all the required info and data.

19 hours ago

We'll send the data as the transaction will be confirmed in the Blockchain.

18 hours ago

Here is your data:

mega.nz



16 hours ago

The decryptor is being prepared now.

16 hours ago

[ 108kB ]

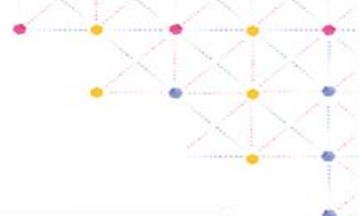
[decryptor.exe](#)

16 hours ago

Decryptor:

- 1) Launch the decryptor under Administrative rights
- 2) Wait till the decryptor window is closed
- 3) if any of the files haven't changed the extension back to the original - repeat 1 and 2

16 hours ago



We have penetrated your network using email compromise. So, first of all - provide all your employees with strict instructions regarding security measures.

Basic recommendations regarding network:

1. Implement better email filtering policies
2. Implement better password policies
3. Consider blocking some particular attacks like pass-the-hash and pass-the-ticket
4. Update all of your internal systems to the latest versions
5. Review network segmentation and take care about buying hardware firewalls with filtering policies
6. Block kerberoasting attacks
7. Conduct full penetrations tests (both external and internal)
8. Implement better AV/EDR systems
9. Review group policies, remove domain and local admin rights for some users.
10. Implement better DLP software system



5 days ago



# CONTI NEWS

If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

[Web mirror](#)[Tor mirror](#)

## “GLENBROOK AUTOMOTIVE G...

<http://glenbrookautomotivegroup.com>

(260) 484-1533  
100 W Coliseum Blvd  
Fort Wayne, IN 46805

Glenbrook Automotive Group, LLC is an automotive company based out of 100 West Coliseum Boulevard, Fort Wayne, Indiana, United States.

10/20/2021

2295

READ MORE >>

## “CREATIVE EXTRUDED PRODU...

<http://creativeextruded.com>

1414 Commerce Park Drive  
Tipp City, Ohio 45371 USA

Phone 800-273-1535 or  
937-667-4485  
Fax 937-667-3647

Creative Extruded Products is a precision custom profile extrusion and injection molding company, specializing in small to medium sized profiles as well as molded components. Since 1979 Creative has developed an innovative, experienced staff capable of developing the extrusion and injection molding systems to solve your problems. Our experience has developed capabilities ranging from the extrusion, injection molding, and fabrication.

PUBLISHED 10%

10/20/2021

90

READ MORE >>

## “JVCKENWOOD”

<http://www.jvckenwood.com>

3-12, Moriyacho, Kanagawa-ku,  
Yokohama-shi  
Kanagawa  
221-0022  
Japan

JVCKenwood focuses on car and home electronics, wireless systems for the worldwide consumer electronics market, professional broadcast, CCTV and digital and analogue two-way radio equipment and systems.

PUBLISHED 25%

10/19/2021

596

READ MORE >>

# Referanslar

- <https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis>

**Thank you!**  
**Any Questions?**



[www.prplbx.com](http://www.prplbx.com)