INFORMACIJSKA VARNOST V SLOVENIJI

gorazd.bozic@cert.si, @gbozic
KARL ERJAVEC
MINISTER ZA Zunanje Zadeve
POSLEDICE OKUŽB
Število letno obravnavanih incidentov na SI-CERT

- Tehnični napadi
- Phishing
- Spletne goljufije
- Drugo
- širjenje preko SMB (ETERNALBLUE)
- stikalo za izklop
- neenakomerna porazdelitev po državah
- vstopni vektor: ukrajinski program MEDoc
NOTPETYA

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files. Keep calm, you won't be able to recover your files without our decryption service.

We are not logically capable of restoring your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   MN6N8x117t78mGsdzaAtNbBWX

2. Send us an e-mail with your transaction key to e-mail wowsh@th123456eposted.net. Your personal installation key:

   Q7Ye6-YqIP5D-MuGcXe-7D4TW724-RH49Se-BR58-P-i54Dba-G978xM-t474gP-bSVJhU

If you already purchased your key, please enter it below.

Key: _
Subject: Ransom request: DDoS Attack

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [ANONYMISED] will be DDoS-ed starting Monday, October 9th. if you don't pay 4 Bitcoins @ 1HKyMVGH5jvAMx5ebnhqD3y8HbqeRSoDhq

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([ANONYMISED]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a joke. Check your logs!

If you don't pay by October 9th, attack will start, price to stop will increase to 10 BTC and will go up 2 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful, our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 4 BTC @ 1HKyMVGH5jvAMx5ebnhqD3y8HbqeRSoDhq

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

--
Armada Collective
PHISHING 2017

- na slo. strežniku 59%
- tarče slo. up. 41%

- vseh 193
- PayPal 24
- Apple 16
- Telekom 10
HitBTC is the most advanced Bitcoin exchange

Safe and secure
2-factor authentication, advanced encryption technology, cold storage – we give you peace

Fast, responsive and feature-packed
Our terminal is built on the best technology and lets you trade effortlessly any of the

Robot-friendly API
Make the most out of your trading bot with our leading API and its low latency data and
ICO phishing
VSE KRIPTO FINTE?
zlonamerna koda
From: FINANCNA UPRAVA REPUBLIKE SLOVENIJE [mailto:gfu.fu@gov.si]
Sent: Thursday, August 10, 2017 12:59 PM
To: ___________________________
Subject: Davčna izvršba

Na podlagi tretje točke prvega odstavka 13. člena Zakona o davčnem postopku -YDavP-2 (Uradni list RS, št. 117/06, 24/08
- YDDKIS, 125/08, 20/9 -YDoh-2D, 110/09 (1/10 popr.), 43/10 in 97/101,
ki odloča, da ima zavezanec za davek pravico do podatkov o stanju svojih davčnih obveznosti.
Pozivamo vas, da ste dolžni znesek in pripadajoče zamudne obresti, zaračunane do vključno dneva plačila, poravnati takoj.
Vse ostale informacije se nahajajo v pripomki.

Postopek vodil/-a;
Vesna Bergant
Finančni kontrolor

Furs.xls
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA FINANCE
FINANČNA UPRAVA REPUBLIKE SLOVENIJE

Šmartinska cesta 55, p.p. 631, 1001 Ljubljana

T: 01 478 38 00
F: 01 478 39 00
E: gfu.fu@gov.si

Opomin pred davčno izvršbo – FURS

FURS z opominom poziva zavezanca, da ste dolžni znesek, vključno s pripadajočimi zamudnimi obrestmi, obračunanimi do dneva plačila, plača na posamezne podračune, v skladu s Pravilnikom o podračunih ter načinu plačevanja obveznih dajatev in drugih javnofinančnih prihodkov (Uradni list RS, št. 103/10, 48/11, (51/11 popr.) in 102/12).
Zagon makra, ki se nahaja v datoteki Furs.xlsm

Zagon powershell funkcije Start-Negotiate

LANSIRNIK

Button244 Click()

POGAJALEC (PAYLOAD)

STREŽNIK NAPADALCA

Pošiljanje podatkov o sistemu na strežnik (ip naslov, operacijski sistem, vloga uporabnika, id trenutnega procesa pod katerim teče powershell)

Računalnik dobi vlogo agenta, kar pomeni, da lahko napadalec z njim upravlja (zbira statistiko in podatke ter zaganja ukaze v ukazni lupini)
Priloženo FYI

RS_TRANS_000
431.jar
<table>
<thead>
<tr>
<th>Date</th>
<th>Org</th>
<th>Category</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Artifacts dropped</td>
<td>filename</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Artifacts dropped</td>
<td>filename</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Artifacts dropped</td>
<td>filename</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Artifacts dropped</td>
<td>malware-sample: Windows7187367379786797001.dll 0b7b52302c88c5df59d60dd97e3abcdaf</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Artifacts dropped</td>
<td>malware-sample: BmLgmUUTwdxs1867605313645327118.exe 0916061a5e52701b53210ab2574b122b9b46744</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Artifacts dropped</td>
<td>malware-sample: BmLgmUUTwdxs1867605313645327118.exe b257a2a33e2f3bb881b807440a8f255</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Network activity</td>
<td>hostname: webmail.illida-eng.gr</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Network activity</td>
<td>ip-dst: 185.145.45.70</td>
</tr>
<tr>
<td>2017-07-18</td>
<td></td>
<td></td>
<td>Payload delivery</td>
<td>attachment: RS_TRANS_000431.jar</td>
</tr>
</tbody>
</table>
public static byte[] Decrypt(byte[] encData) throws Exception {
    byte[] simKey = "j8h34lan8qgdm1b9".getBytes("UTF-8");
    byte[] saltBytes = "mp8bn260qykda5bf".getBytes("UTF-8");
    SecretKeySpec secretKeySpec = new SecretKeySpec(simKey, "AES");
    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    IvParameterSpec IVspec = new IvParameterSpec(saltBytes);
    cipher.init(2, (Key)secretKeySpec, IVspec);
    return cipher.doFinal(encData);
}

https://slo-tech.com/novice/t694978/49
Roles & Relations

discoverer

reporter

discoverer

vendor

coordinator

general public  media  law-enforcement  customers
Estonia Cancels 760,000 Electronic ID Cards Because of Crypto Flaw

By Catalin Cimpanu

Estonian authorities have decided to block and disable over 760,000 national electronic ID cards due to a cryptographic vulnerability that could allow attackers to clone IDs and forge identities.