

BAD RABBIT – Ransomware

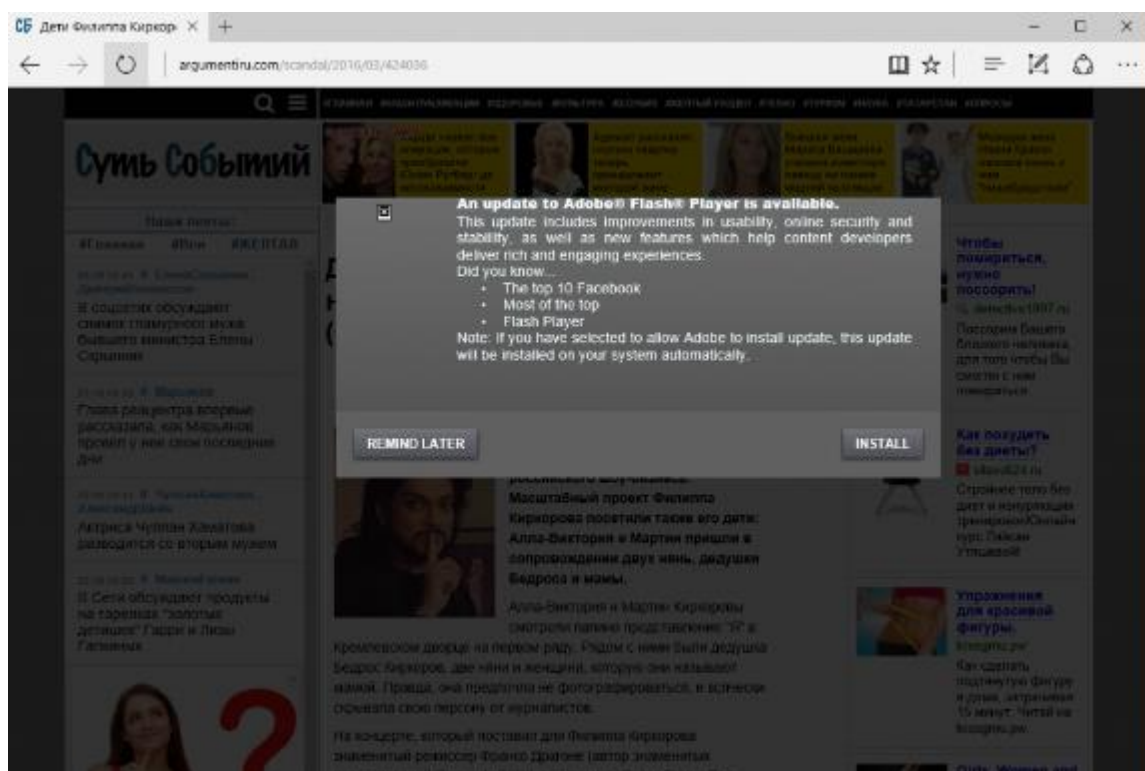
Ein weiterer Not-Petya-Ableger



Eine neue Bedrohung im Netz – die Ransomware „BAD RABBIT“

Der kürzlich im Netz aufgetauchte Not-Petya-Ableger verschlüsselte am vergangenen Dienstag zahlreiche Endgeräte im Bereich Russland und Ukraine.

Die Ransomware wird per Drive-By-Download auf einer Website (Liste betroffener Seiten anbei) ausgeteilt, getarnt als vermeintlich sicherer Download für eine neue Version des Adobe Flash-Players.



Die als Flashplayer-Update getarnte Schadsoftware „Bad Rabbit“

Beim Klick auf den unscheinbaren „install“-Button lädt das Script einen Filecoder von der URL `hxxp://1dnscontrol[.]com/flash_install.php` herunter, welcher die Daten auf dem Datenträger verschlüsselt.

Das Endgerät ist nun nicht mehr nutzbar und die Dateien sind verschlüsselt.

Der Preis für die Entschlüsselung

Das geforderte Lösegeld, um seine Daten entschlüsseln zu können, beträgt aktuell 0,05BTC (Bitcoin). Dies entspricht nach aktuellem Kurs in etwa 230€. Wird das Zahlungsziel von 40 Stunden nicht eingehalten, erhöht sich der Betrag.

Mit dieser Methode soll das Opfer unter Druck gesetzt werden, impulsiv schneller zu handeln und das Lösegeld zu bezahlen.

```
Dops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

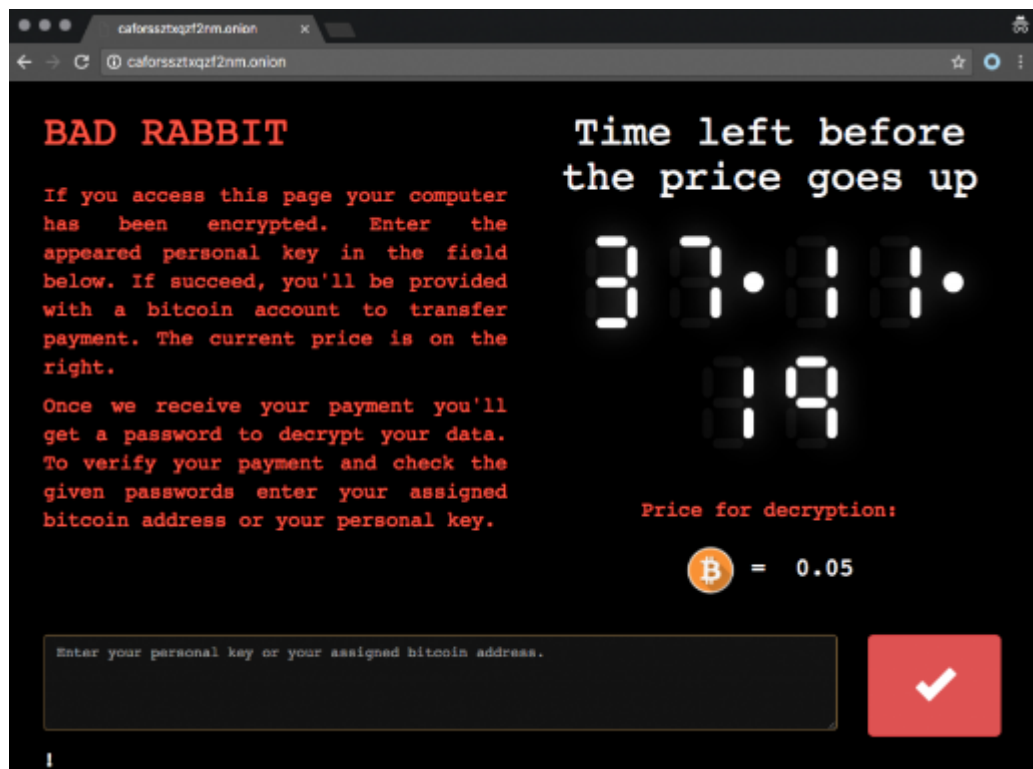
Your personal installation key#1:

ZORqoZdoI+vr6yMqMlccRe/TmI+r+JNFx60Up2d+RHZ67xJ2b/5/UU5bzvMQkRSX
FF3rcIQIXAD1HoaAcxCTupQyW9UyGnkIFxP35vszHqArN7/MEWtXb8bb7BMSbJx8
6thxli0FSIRUPr+IZXm2tR938ohkDAhJMkroU+xBLBylqgScJGN1UXL44j7HcLJi
Ba3a/AC0Sg.jb4tsGfXUTFft19Muik6UnLgoz4XAYwgWYJLPD/69P7Jq80AUJyExN
EKheR2bz17LrpUcrg6DfnT4qE5J3I0PErfE/3fxLhc20293tcwhGrNinxsf4bL81
7M02LsCle0UNG/NgH1qK05SUpBAMiqY9Ug==

If you have already got the password, please enter it below.
Password#1: _
```

Notifikation, nachdem das System verschlüsselt wurde

Damit aber nicht genug. Die Ransomware verbreitet sich über SMB (Server Message Block) über das Netzwerk und infiziert weitere Geräte.



Die Zahlungsseite setzt ihre Opfer zeitlich unter Druck

Wir raten davon ab, das Lösegeld zu bezahlen

Einer der Gründe, warum der Einsatz von Ransomware so boomt ist, dass viele Opfer nachgeben und das Lösegeld bezahlen. Eine Garantie, dass dadurch die Daten wiederhergestellt werden, gibt es nicht. Wir raten stets dazu, eine Backup-Strategie zu fahren und sein Netzwerk prophylaktisch mit einer Gateway-Security, wie einem Antivirus auf dem Endpoint auszustatten.

Zudem kann hier zur Prevention Vorarbeit in den Firewall-Regeln getroffen werden.

Prophylaktisch sollte der Zugang zu folgenden Adressen gesperrt werden:

C&C servers

Payment site: [http://caforssztxqzf2nm\[.\]onion](http://caforssztxqzf2nm[.]onion)

Inject URL: [http://185.149.120\[.\]3/scholargoogle/](http://185.149.120[.]3/scholargoogle/)

Distribution URL: [http://1dnscontrol\[.\]com/flash_install.php](http://1dnscontrol[.]com/flash_install.php)

List of compromised sites:

- hxxp://argumentiru[.]com
- hxxp://www.fontanka[.]ru
- hxxp://grupovo[.]bg
- hxxp://www.sinematurk[.]com
- hxxp://www.aica.co[.]jp
- hxxp://spbvoditel[.]ru
- hxxp://argumenti[.]ru
- hxxp://www.mediaport[.]ua
- hxxp://blog.fontanka[.]ru
- hxxp://an-crimea[.]ru
- hxxp://www.t.ks[.]ua
- hxxp://most-dnepr[.]info
- hxxp://osvitaportal.com[.]ua
- hxxp://www.otbrana[.]com
- hxxp://calendar.fontanka[.]ru
- hxxp://www.grupovo[.]bg
- hxxp://www.pensionhotel[.]cz
- hxxp://www.online812[.]ru
- hxxp://www.imer[.]ro
- hxxp://novayagazeta.spb[.]ru
- hxxp://i24.com[.]ua
- hxxp://bg.pensionhotel[.]com
- hxxp://ankerch-crimea[.]ru

Quelle: welivesecurity / ESET Deutschland GmbH, <https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/>