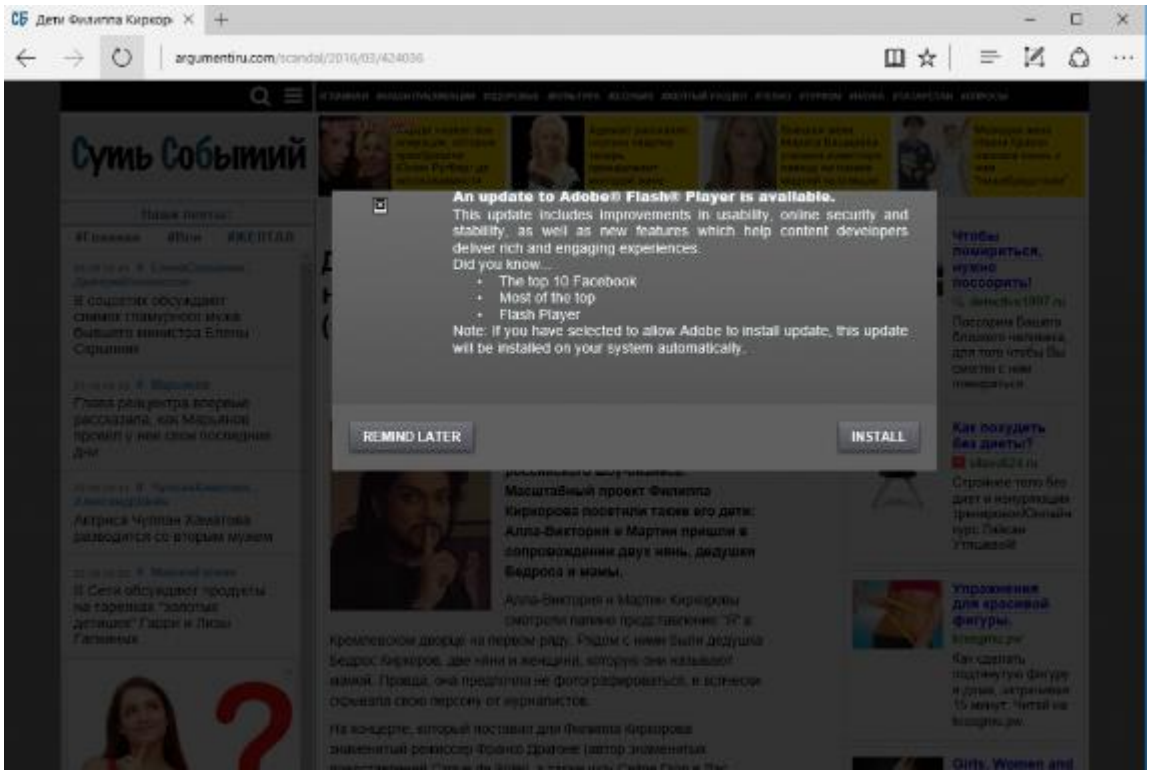
BAD RABBIT – Ransomware

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.

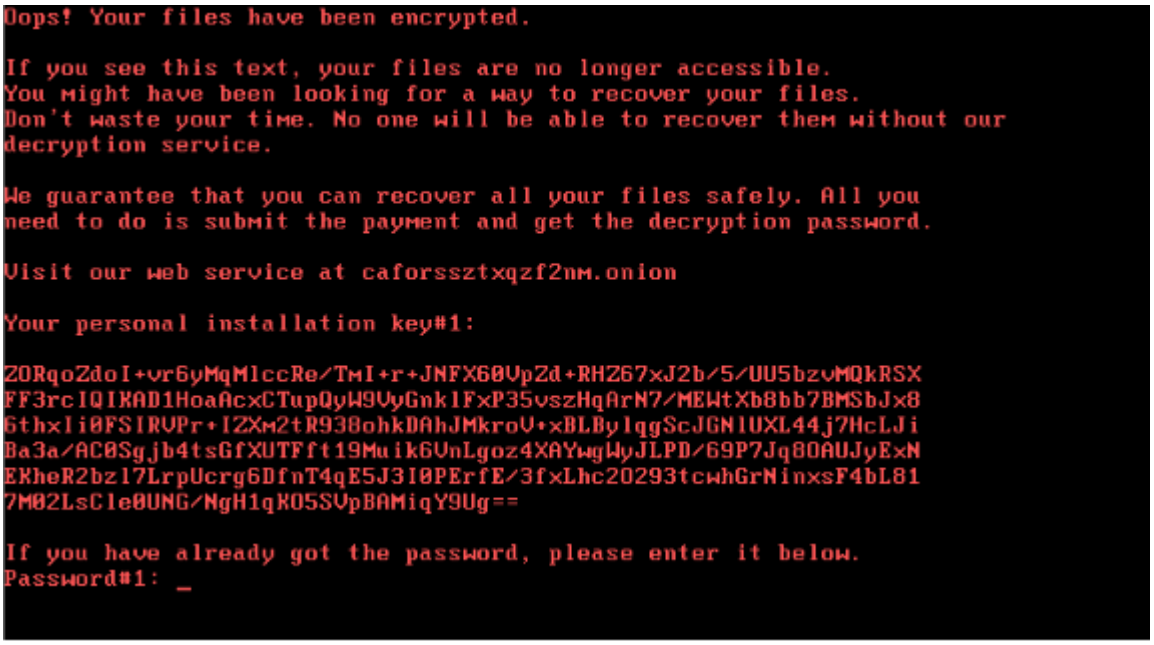
Das Endgerät ist nun nicht mehr nutzbar und die Dateien sind verschlüsselt.

TAROX Aktiengesellschaft | Stellenbachstr. 49–51 | 44536 Lünen | Telefon: +49 (0) 231 / 98 98 0-0 | Telefax: +49 (0) 231 / 98 98 0-101 | info@tarox.de

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.



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.

TAROX Aktiengesellschaft | Stellenbachstr. 49–51 | 44536 Lünen | Telefon: +49 (0) 231 / 98 98 0-0 | Telefax: +49 (0) 231 / 98 98 0-101 | info@tarox.de

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 Firewalll-Regeln getroffen werden.

Prophylaktisch sollte der Zugang zu folgenden Adressen gesperrt werden:

C&C servers

Payment site: http://caforssztxqzf2nm[.]onion

Inject URL: http://185.149.120[.]3/scholargoogle/

Distribution URL: hxxp://1dnscontrol[.]com/flash_install.php

TAROX Aktiengesellschaft | Stellenbachstr. 49–51 | 44536 Lünen | Telefon: + 49 (0) 231 / 98 98 0-0 | Telefax: + 49 (0) 231 / 98 98 0-101 | info@tarox.de

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/

TAROX Aktiengesellschaft | Stellenbachstr. 49–51 | 44536 Lünen | Telefon: +49 (0) 231 / 98 98 0-0 | Telefax: +49 (0) 231 / 98 98 0-101 | info@tarox.de