Abstract

This threat advisory provides analysis by Radware's Emergency Response Team (ERT) of the ransomware campaign that broke out on October 24, 2017 and is impacting organizations across Eastern Europe.

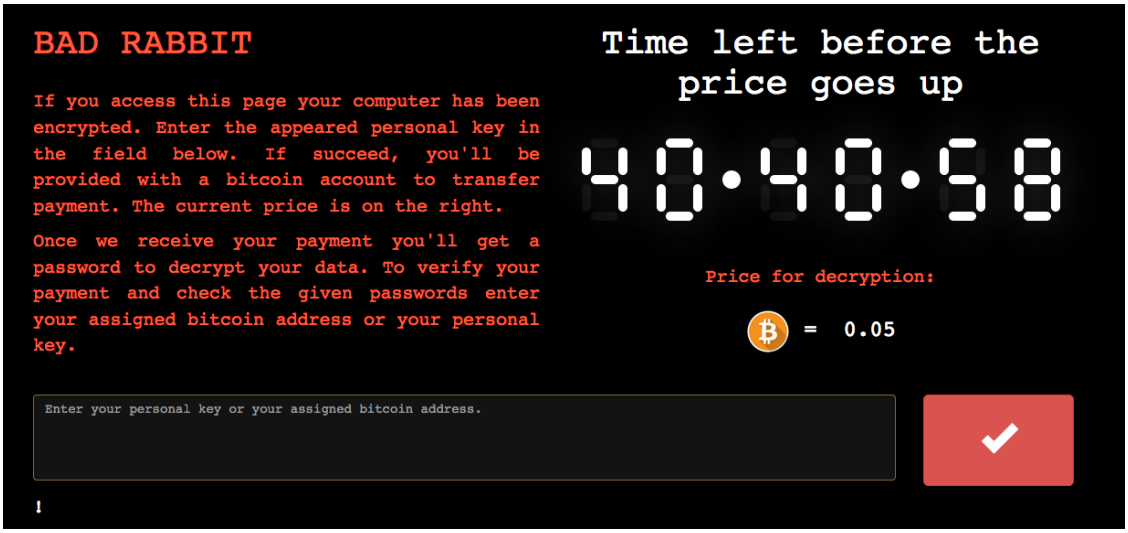

Figure 1: BadRabbit payment page

BadRabbit

BadRabbit follows previous ransomware operations such as WannaCry and Nyetya (a.k.a. NotPetya). At the moment, BadRabbit resembles the Nyetya campaign as it uses the original Petya ransomware variant. As many organizations update and patch their security solutions following such attacks, BadRabbit authors created a variant that does not include a memory-wiping component like in the Nyetya campaign. BadRabbit leverages the EternalRomance exploit to propagate laterally across a network, another vulnerability that was released by Shadow Brokers and addressed in the Microsoft MS17-010 security bulletin.

Distribution

BadRabbit was distributed via a fake flash update that required user interaction. When visiting one of the compromised sites, a user is presented with a popup for a flash update. This fake flash update was delivered to a user via download while viewing a compromised website. These websites were compromised with a piece of malicious JavaScript that was injected into their HTML body or on one of their .js files. Users were redirected to 1dnscontrol[.]com, the site hosting the malicious file. A POST request is then sent to a static IP address 185.149.120[.]3 with a path to /scholasgoolge. After the POST, the dropper is downloaded onto the user's computer from one of two different paths, index.php or flash_install.php. Users are then redirected to a site that dropped the malware onto their computer.

Infection

The reason why this attack is not sophisticated is due to its dependence on user interaction. Ultimately, the user has to initiate the download by thinking they have to install a flash update. Once the user interacts with the update, a dropper containing BadRabbit is deployed on a user's machine.

Propagation

After the device is infected, an SMB component and WebDAV is used to worm laterally across networks to identify additional devices to compromise. In addition, BadRabbit uses a list of weak credentials and a version of post exploitation hacktool mimikatz to gain further credentials for infection. For the moment, the server hosting the malware has been taken down and is no longer spreading the worm.

Infected Files

.3ds .7z .accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .hpp .hxx .iso .java .jfif .jpe .jpeg .jpg .js .kdbx .key .mail .mdb .msg .nrg .odc .odf .odg .odi .odm .odp .ods .odt .ora .ost .ova .ovf .p12 .p7b .p7c .pdf .pem .pfx .php .pmf .png .ppt .pptx .ps1 .pst .pvi .py .pyc .pyw .qcow .qcow2 .rar .rb .rtf .scm .sln .sql .tar .tib .tif .tiff .vb .vbox .vbs .vcb .vdi .vfd .vhd .vhdx .vmc .vmdk .vmsd .vmtm .vmx .vsdx .vsv .work .xls .xlsx .xml .xvd .zip

Default Credentials for Brute Forcing

Usernames

Administrator, Admin, Guest, User, User1, user-1, Test, root, buh, boss, ftp, rdp, rdpuser, rdpadmin, manager, support, work, other user, operator, backup, asus, ftpuser, ftpadmin, nas, nasuser, nasadmin, superuser, netguest, alex

Passwords

Administrator, administrator, Guest, guest, User, user, Admin, adminTest, test, root, 123, 1234, 12345, 123456, 1234567, 12345678, 123456789, 1234567890, Administrator123, administrator123, Guest123, guest123, User123, user123, Admin123, admin123Test123, test123, password, 111111, 55555, 77777, 777, qwe, qwe123, qwe321, qwer, qwert, qwerty, qwerty123, zxc, zxc123, zxc321, zxcv, uiop, 123321, 321,love, secret, sex, god

Domains

Compromised Websites

- 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

Payment Page

- hxxp://caforssztxqzf2nm[.]onion

Inject URL

- hxxp://185.149.120[.]3/scholargoogle/

Distribution URL

- hxxp://1dnscontrol[.]com/flash_install.php
- hxxp://1dnscontrol[.]com/index.php

How to Prepare

- Make employees aware at the organization. They should understand how this threat works and be conscious to malicious activity.
- Perform regular backups of all critical information to limit the impact of data or system loss. Ideally, critical information should be kept on a separate device, and backups should be stored offline.
- Maintain updated anti-virus software.
- Make sure you have a strong anti-malware solution which is constantly updated with new signatures and new types of malware. It should be deployed on all workstations and laptops.
- Keep your operating system and software updated with the latest patches.
- Do not follow unsolicited links in email.
- Use caution when opening email attachments.
- Follow safe practices when browsing the web.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.