BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

25.10.2017

İNCELEME DOKÜMANI

BADRABBIT ZARARLI YAZILIMI

USOM TR-CERT ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

Bilgi Teknolojileri ve İletişim Kurumu (BTK)
Ulusal Siber Olaylara Müdahale Merkezi (USOM)
Adres: Bilgi Teknolojileri ve İletişim Kurumu (BTK) Merkez Binası
Eskişehir Yolu 10.Km No:276 Çankaya/Ankara
Telefon Numarası: +90 312 586 53 05 - 0549 779 87 85
Fax: +90 312 586 54 00
iletisim@usom.gov.tr

Genel Bilgi

Dünya genelinde kendisini 'Adobe Flash Player' güncellemesi olarak göstererek BadRabbit adlı ransomware zararlı yazılımı sistemlere bulaşmaktadır. İlgili zararlı yazılım sisteme indirilen zararlı bir dosya ile bulaşıp tüm dosyaları şifreleyerek açılması için ücret talep etmektedir. Zararlı yazılım bulaştığı sistemler üzerinden edindiği ve zararlı yazılımda tanımlı olan kullanıcı adı parola bilgilerini kullanarak iç ve dış ağlarda SMB servisi üzerinden yayılmaktadır.

Zararlı Yazılım Detayları

Zararlı yazılım çalıştırıldığında aşağıdaki dosya bilgileri yer alan zararlıları oluşturmaktadır.

Zararlı Yazılım Tanımlayıcı Bilgileri

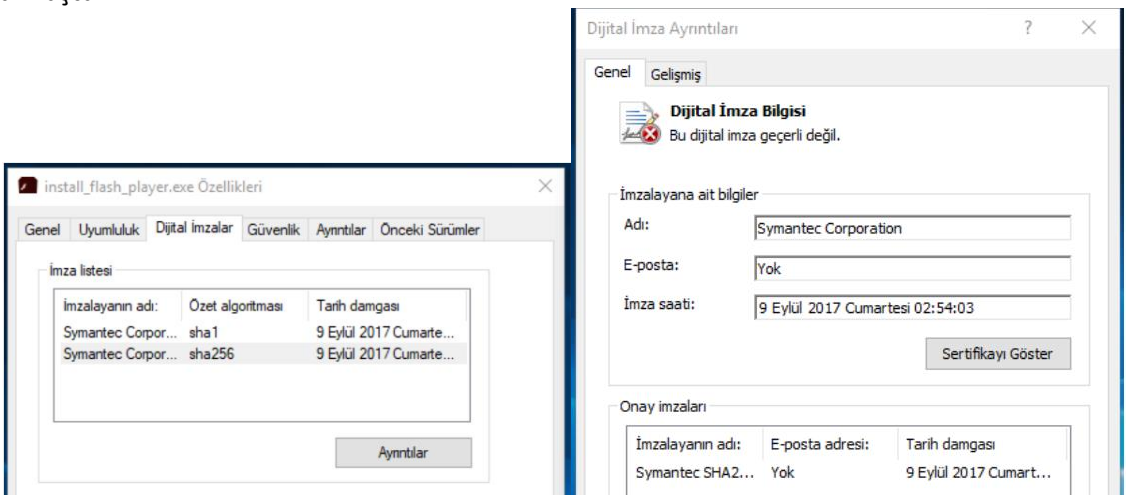
Dosya ismi:	install_flash_player.exe
Dosya türü:	PE32 executable (console) Intel 80386, for MS Windows
Dosya boyutu:	431.5KB
Dosya dizini:	-
İlişkili dosyalar:	-
Özetleme MD5:	fbbdc39af1139aebba4da004475e8839
Özetleme SHA1:	de5c8d858e6e41da715dca1c019df0bfb92d32c0
Özetleme SHA256:	630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

Dosya ismi:	infpub.dat
Dosya türü:	Data
Dosya boyutu:	401.1KB
Dosya dizini:	C:\Windows\infpub.dat
İlişkili dosyalar:	install_flash_player.exe, rundll32.exe
Özetleme MD5:	c4f26ed277b51ef45fa180be597d96e8
Özetleme SHA1:	e9efc622924fb965d4a14bdb6223834d9a9007e7
Özetleme SHA256:	14d82a676b63ab046ae94fa5e41f9f69a65dc7946826cb3d74cea6c030c2f958

Dosya ismi:	cscc.dat
Dosya türü:	PE32 executable (native) Intel 80386, for MS Windows
Dosya boyutu:	177.2KB
Dosya dizini:	C:\Windows\cscc.dat
İlişkili dosyalar:	rundll32.exe
Özetleme MD5:	b4e6d97dafd9224ed9a547d52c26ce02
Özetleme SHA1:	59cd4907a438b8300a467cee1c6fc31135757039
Özetleme SHA256:	682adcb55fe4649f7b22505a54a9dbc454b4090fc2bb84af7db5b0908f3b7806

Dosya ismi:	dispci.exe
Dosya türü:	PE32 executable (console) Intel 80386, for MS Windows
Dosya boyutu:	139.5KB
Dosya dizini:	C:\Windows\dispci.exe
İlişkili dosyalar:	rundll32.exe
Özetleme MD5:	b14d8faf7f0cbcfad051cefe5f39645f
Özetleme SHA1:	afeee8b4acff87bc469a6f0364a81ae5d60a2add
Özetleme SHA256:	8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93

Zararlı yazılımın özellikleri incelendiğinde geçerli olmayan bir sertifika ile aşağıdaki şekilde imzalandığı görülmüştür.



Sertifika bilgileri

Gerçekleştirilen statik ve dinamik kod analizleri sonucunda aşağıdaki bilgilere ulaşılmıştır:

SMB servisi üzerinden "infpub.dat" dosyasında ön tanımlı olan kullanıcı adı/parola çiftleri iç ve dış ağlarda denenmektedir. Bu kullanıcı adı parolalar aşağıdaki gibidir:

- Kullanıcı adı:

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

- Parola:

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

No.	Time	Source	Destination	Protocol	Length	Info
1610	16.484005	172.30.101.150	40.77.229.67	TCP	66	[TCP Retransmission] 49841 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1097	10.484051	172.30.101.150	40.77.229.67	TCP	66	[TCP Retransmission] 49841 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1622	16.499680	172.30.101.150	40.113.8.255	TCP	66	[TCP Retransmission] 49840 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1099	10.484082	172.30.101.150	40.113.8.255	TCP	66	[TCP Retransmission] 49840 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4149	57.914873	172.30.101.152	172.30.101.150	SMB	339	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
4145	57.911940	172.30.101.152	172.30.101.150	SMB	339	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
4060	56.034104	172.30.101.152	172.30.101.150	SMB	339	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
4151	57.915908	172.30.101.152	172.30.101.150	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
4147	57.913323	172.30.101.152	172.30.101.150	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
4062	56.037239	172.30.101.152	172.30.101.150	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
4148	57.914558	172.30.101.150	172.30.101.152	SMB	162	Session Setup AndX Request, NTLMSSP_NEGOTIATE
4144	57.911606	172.30.101.150	172.30.101.152	SMB	162	Session Setup AndX Request, NTLMSSP_NEGOTIATE
4059	56.033455	172.30.101.150	172.30.101.152	SMB	162	Session Setup AndX Request, NTLMSSP_NEGOTIATE
4150	57.915412	172.30.101.150	172.30.101.152	SMB	532	Session Setup AndX Request, NTLMSSP_AUTH, User: WIN10X64\USOM
4146	57.912652	172.30.101.150	172.30.101.152	SMB	532	Session Setup AndX Request, NTLMSSP_AUTH, User: WIN10X64\USOM
4061	56.035232	172.30.101.150	172.30.101.152	SMB	532	Session Setup AndX Request, NTLMSSP_AUTH, User: WIN10X64\USOM
4058	56.021761	172.30.101.152	172.30.101.150	SMB	143	Negotiate Protocol Response
4057	56.021028	172.30.101.150	172.30.101.152	SMB	213	Negotiate Protocol Request
5674	87.541467	172.30.101.150	172.30.101.20	TCP	66	49930 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4097	56.270755	172.30.101.150	172.30.101.151	TCP	66	49904 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4054	56.020560	172.30.101.150	172.30.101.152	TCP	66	49902 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4772	71.268955	172.30.101.150	172.30.101.152	TCP	54	49902 → 445 [RST, ACK] Seq=1918 Ack=1062 Win=0 Len=0
4072	56.081334	172.30.101.150	172.30.101.152	TCP	54	49902 → 445 [ACK] Seq=746 Ack=414 Win=525056 Len=0
4153	57.956294	172.30.101.150	172.30.101.152	TCP	54	49902 → 445 [ACK] Seq=1918 Ack=1062 Win=524288 Len=0
4056	56.020918	172.30.101.150	172.30.101.152	TCP	54	49902 → 445 [ACK] Seq=1 Ack=1 Win=525568 Len=0
3841	55.184167	fe80::bd98:4ebc:86e…	fe80::9cd0:b643:50e…	TCP	86	49900 → 445 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
3824	55.181877	172.30.101.150	195.175.115.56	TCP	66	49899 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3823	55.181852	172.30.101.150	172.30.101.1	TCP	66	49898 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2444	34.303667	172.30.101.150	204.79.197.200	TCP	66	49883 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1482	15.375187	172.30.101.150	172.30.101.2	TCP	66	49857 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1161	11.359714	172.30.101.150	172.30.101.1	TCP	66	49854 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
877	7.471296	172.30.101.150	40.77.229.53	TCP	66	49845 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
876	7.471230	172.30.101.150	192.168.105.43	TCP	66	49844 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
875	7.470186	172.30.101.150	191.237.218.239	TCP	66	49843 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
874	7.470075	172.30.101.150	80.239.244.114	TCP	66	49842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
872	7.469903	172.30.101.150	40.77.229.67	TCP	66	49841 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Zararlı yazılım tarafından oluşan ağ trafiği

Ayrıca zararlı yazılımın hedef sistemdeki bellek üzerinde bulunan kullanıcı adı parola bilgilerini elde ederek (Mimikatz benzeri), ağdaki diğer bilgisayarlara yayılabildiği görülmüştür.

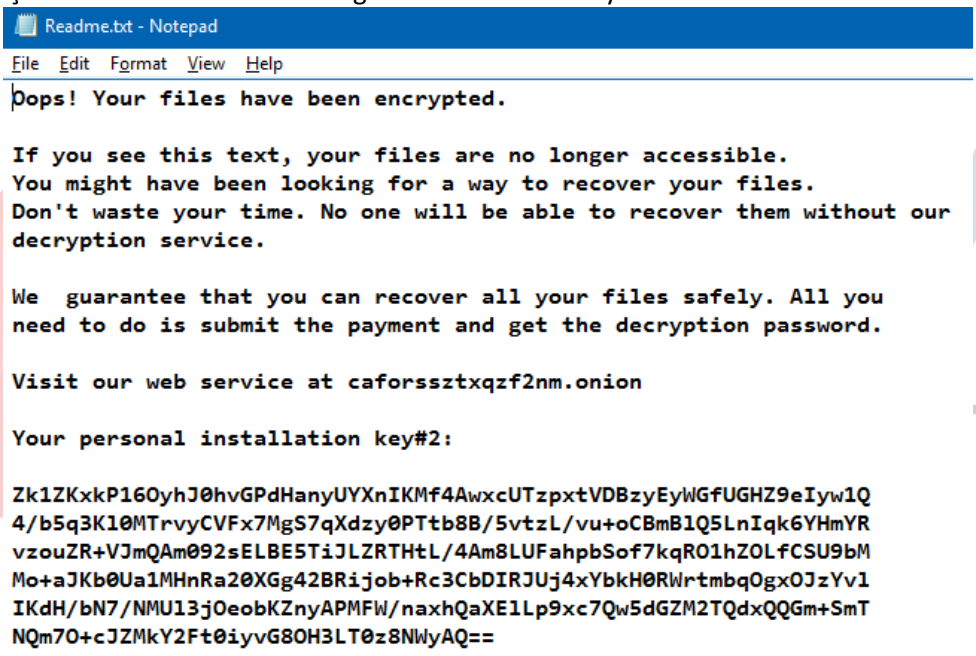
No.	Time	Source	Destination	Protocol	Length	Info
10212	347.493331	172.30.101.151	172.30.101.152	SMB	132	Tree Connect AndX Request, Path: \\172.30.101.152\ADMIN$
10213	347.493750	172.30.101.152	172.30.101.151	SMB	107	Tree Connect AndX Response
10214	347.493830	172.30.101.151	172.30.101.152	SMB	150	NT Create AndX Request, Path: cscc.dat
10215	347.494130	172.30.101.152	172.30.101.151	SMB	93	NT Create AndX Response, FID: 0x0000, Error: STATUS_OBJECT_NAME_NOT_FOUND
10216	347.494204	172.30.101.151	172.30.101.152	SMB	152	NT Create AndX Request, FID: 0x400d, Path: infpub.dat
10217	347.496170	172.30.101.152	172.30.101.151	SMB	193	NT Create AndX Response, FID: 0x400d
10218	347.496260	172.30.101.151	172.30.101.152	SMB	1142	Write AndX Request, FID: 0x400d, 1024 bytes at offset 0
10219	347.496753	172.30.101.152	172.30.101.151	SMB	105	Write AndX Response, FID: 0x400d, 1024 bytes
10220	347.496835	172.30.101.151	172.30.101.152	SMB	1142	Write AndX Request, FID: 0x400d, 1024 bytes at offset 1024
10221	347.496975	172.30.101.152	172.30.101.151	SMB	105	Write AndX Response, FID: 0x400d, 1024 bytes
10222	347.497050	172.30.101.151	172.30.101.152	SMB	1142	Write AndX Request, FID: 0x400d, 1024 bytes at offset 2048

Başarılı yayılma girişimi

Aynı dosya içerisinde yer alan bilgilere göre şifrelenen dosya uzantıları aşağıdaki gibidir:

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

Şifreleme işlemi sonrası son kullanıcı bilgilendirilmekte ve fidye istenmektedir.



Fidye mesajı

Zararlı Yazılım Bulaşma ve Yayılma Senaryosu

1. ‘Adobe Flash Player’ güncellemesi gibi görünen çalıştırılabilir dosya (install_flash_player.exe) son kullanıcı hatası sonucu hedef sisteme indirilir ve çalıştırılır. Çalışan yazılım yetkili kullanıcı hakları talep eder.
2. “C:\Windows\” dizini altında “infpub.dat”, “cscc.dat” ve “dispci.exe” dosyaları oluşturulur. Bu dosyalar aracılığı ile hedef sistem üzerinde ilgili dosya uzantıları şifrelenir.
3. Bellek üzerindeki kullanıcı adı parola bilgileri elde edilir (Mimikatz benzeri).
4. SMB servisi üzerinden yayılmak için zararlı yazılım içerisinde gömülü olarak gelen ve bellek üzerinden elde ettiği kullanıcı adı parola ikililerini kullanır. Başarılı olduğu durumda süreç tekrarlanır.
5. Hedef sistem üzerinde boot ayarları değiştirip uyarı çıkartarak ve “C:\” dizininde “Readme.txt” isimli not oluşturularak son kullanıcıdan fidye istenir.

Alınması Gereken Önlemler

Zararlı Yazılım Bulaşmasına Karşı Alınacak Önlemler

- Güvenli olmayan kaynaklardan dosya indirilmemesi ve çalıştırılmaması
- Son kullanıcılarda 'local admin' yetkisine sahip kullanıcıların kullanılmaması
- Basit parola ve jenerik kullanıcı isimlerinin kullanılmaması
- Sistemlerin yama yönetiminin düzenli uygulanması
- Antivirüs yazılımı kullanımı (Çeşitli antivirüs yazılımlarının söz konusu zararlı yazılımı engellediği bilindiğinden, son kullanıcı makinaları ve sunucularda antivirüs yazılımlarının aktif ve tanımlarının güncel tutulması)
- WMIC (Windows Management Instrumentation Command-line) kullanımının engellenmesi

Not: Bazı sistemler WMI farklı amaçlarla kullanılmaktadır, kapatılması farklı sorunlara neden olabilir.

Zararlı Yazılımın Hedef Sistemde Çalışmasına Karşı Alınacak Önlemler

- "C:\Windows\infpub.dat" ve "C:\Windows\cscc.dat" dosyalarının çalışmasını engellemek için, ilgili dosyaların oluşturulması ve yetkilerinin kısıtlanması

(ref:https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware)

- Düzenli yedek alınması
- Shadow dosyaların incelemesi; son kullanıcının zararlı yazılıma 'local admin' yetkisi vermediği durumlarda, son kullanıcı verilerinin kurtarılması için shadow dosyaları kontrol edilebilir.

Zararlı Yazılımın Bulaştığı Hedef Sistemden Yayılmasına Karşı Alınacak Önlemler

- Mimikatz gibi RAM'deki açık tutulan parolaları çıkartan yazılımlara önlem olarak, parolaların açık şekilde tutulmasının engellenmesi
- Farklı sunucu ve son kullanıcı bilgisayarlarında aynı yetkili hesapların (local admin) aynı kullanıcı adı ve parola ile kullanılmaması