Charming Kitten (APT35)

infinitumit.com.tr/apt-35/

infinitumit

June 20, 2022

Charming Kitten (APT35) olarak bilinen APT grubunun İran devleti ile bağlantılı olduğu düşünülmektedir. İnsan hakları aktivitelerine, akademik araştırmacılara ve medya kuruluşlarına karşı İran devletine **Siber İstihbarat** sağladığı, hedeflediği ülkeler arasında Amerika Birleşik Devletleri ve Orta Doğru ülkeleri bulunduğu değerlendirilmektedir.

Charming Kitten hedeflerden en çok bilgi toplayabileceği sistemlere erişmeye çalışmakta; kurumların kullandığı mail adresleri veya kişisel Facebook hesapları bunlardan bazılarıdır.

En Çok Dikkat Çeken Siber Saldırıları:

HBO

2017 yılında, HBO'ya yapılan bir siber saldırının ardından, gizli bilgilerin sızdırıldığı gerekçesiyle geniş çaplı bir ortak soruşturma başlatıldı. Takma adı Skote Vahshat olan bir bilgisayar korsanı tarafından yapılan açıklamaya göre fidye ödenmezse; Game of Thrones bölümleri de dahil olmak üzere televizyon bölümlerinin senaryolarının sızdırılacağı iddia edilmişti. Bir kısmı o sırada yayınlanmayan şovlar ve bölümler olan 1.5 terabayt veri sızıntısına neden olmuştur.

Amerikan Seçimlerine Müdahale

Microsoft'a göre, Ağustos ve Eylül 2019 arasındaki 30 günlük bir süre içinde Charming Kitten, hedeflenen e-posta hesaplarıyla ilgili bilgi edinmek için 2.700 girişimde bulundu. Bu, 241 saldırı ve hacklenmiş 4 hesapla sonuçlandı. Girişimin Amerika Birleşik Devletleri başkanlık kampanyasını hedeflediği düşünülse de ele geçirilen hesapların hiçbiri seçimle ilgili değildi.

Microsoft, özellikle kimin hedef alındığını açıklamadı, ancak Reuters tarafından daha sonra yayınlanan bir rapor, bunun Donald Trump’ın yeniden seçim kampanyası olduğunu iddia etti.

İran Dışişleri Bakanı Mohammad Javad Zarif “Sizin seçiminizde (Amerika Birleşik Devletleri) bu seçime müdahale etme tercihimiz yok” ve “İç seçimlere müdahale etmiyoruz” derken, İran seçime karışmaya herhangi bir müdahaleyi reddetti. Benzer kurban profilleri çok dikkat çekici; akademi, gazetecilik, insan hakları aktivizmi ve siyasi muhalefet alanlarında İran’ı ilgilendiren insanlardı.

APT-35 Tarafından Kullanılan Zararlı Yazılımlar ve Araçları

DownPaper:

Backdoor Trojen olarak kullanılan zararlı yazılımın ana hedefi 2. bir zararlı yazılımı hedef sistem içine indirmek ve çalıştırmaktır.

MITRE ATT&CK Teknikleri

Application Layer Protocol: Web Protocols (T1071):

Hedef cihaz içinden bağlantı almak için HTTP protokolü üzerinden bir C2 kullanılır.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547) :

PowerShell ile Registry içine veri girişi yapar AutoStart özelliği ile sistem içinde kalıcılık sağlar ve her oturum açıldığında zararlı yazılım kendini otomatik olarak başlatır.

Command and Scripting Interpreter: PowerShell (T1059) :

DownPaper zararlısı sistem içinde çalışmak için PowerShell kullanır.

Query Registry (T1012) :

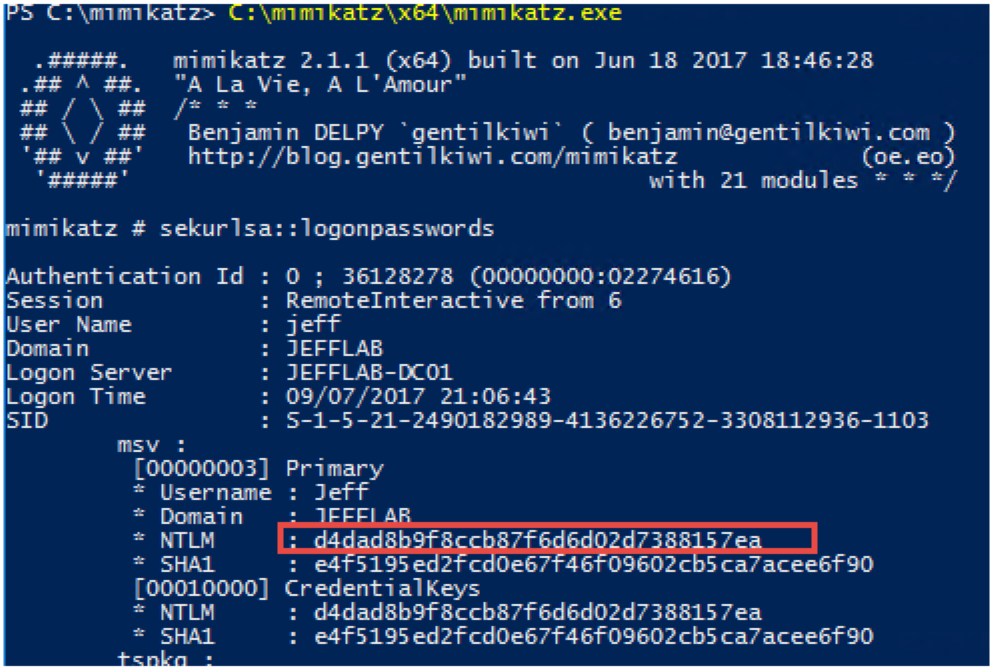
Eski Windows sistemleri üzerinde bulunan güvenlik zafiyetleri Exploit edilebilir olduğu için DownPaper hedef sistem içinde çalıştığı zaman eski sistemleri belirlemek için Registry üzerinden Windows Update bilgilerini okuyor.

System Owner/User Discovery (T1033):

Hedef sistem üzerinde oturum açan kullanıcı adına ait bilgilerini topluyor ve saldırganlar tarafından kullanılan C2 sunucunsa bu bilgiyi yüklüyor.

Mimikatz

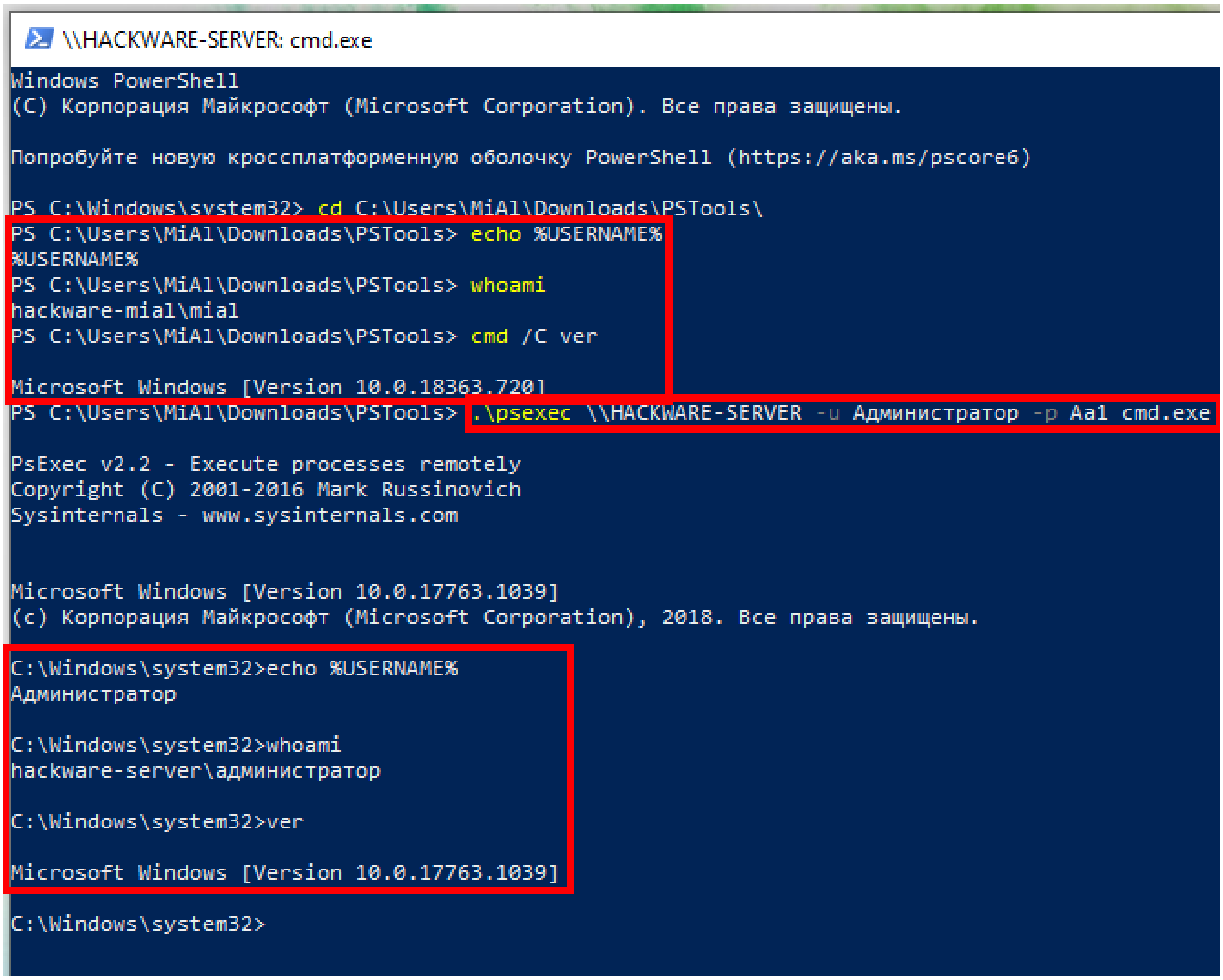
Saldırganlar hedef sistem içinden Windows kullanıcı bilgilerine erişmek için kullandığı bir araç, lsass dump edilerek memory içinden dump edilen veriler Mimikatz ile anlaşılır bir veriye dönüşür.


```
PS C:\mimikatz> C:\mimikatz\x64\mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on Jun 18 2017 18:46:28
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                   with 21 modules * * */

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 36128278 (00000000:02274616)
Session           : RemoteInteractive from 6
User Name         : jeff
Domain            : JEFFLAB
Logon Server      : JEFFLAB-DC01
Logon Time        : 09/07/2017 21:06:43
SID               : S-1-5-21-2490182989-4136226752-3308112936-1103
        msv :
         [00000003] Primary
         * Username : Jeff
         * Domain   : JEFFLAB
         * NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
         * SHA1     : e4f5195ed2fcd0e67f46f09602cb5ca7acee6f90
         [00010000] CredentialKeys
         * NTLM     : d4dad8b9f8ccb87f6d6d02d7388157ea
         * SHA1     : e4f5195ed2fcd0e67f46f09602cb5ca7acee6f90
        tspkg :
```

(Kullanıcıya ait NTLM hash verisi)

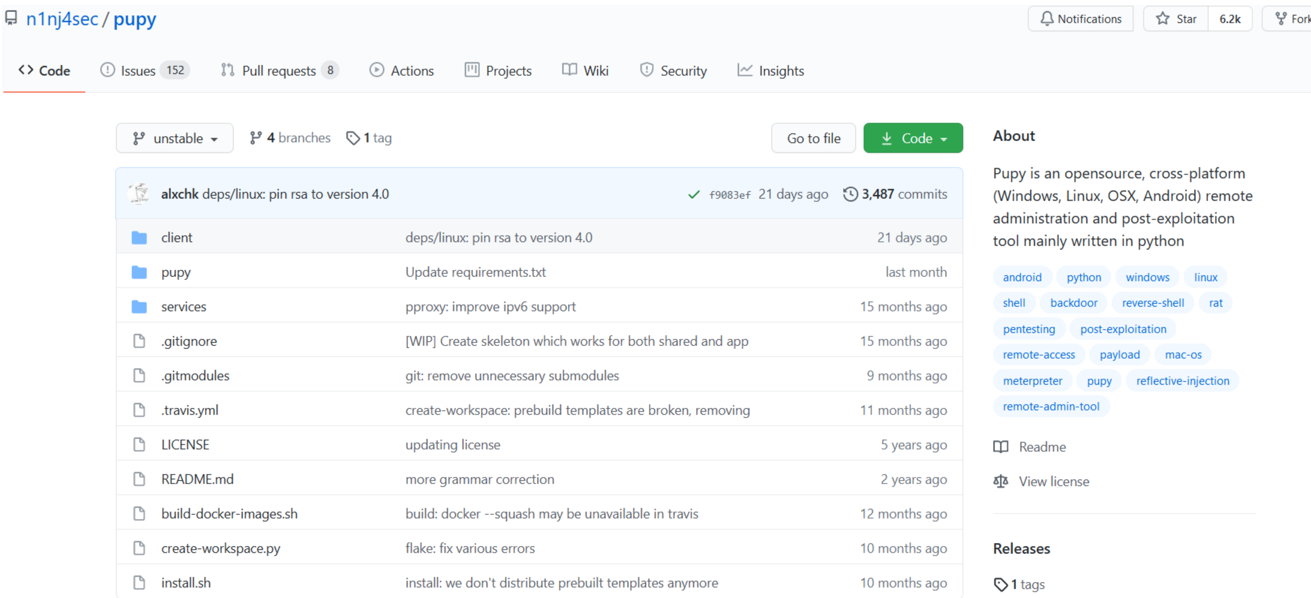
PsExec

PsExec, bir yazılımı aynı ağ içinde fakat başka bir bilgisayarda çalıştırmak için kullanılabilen ücretsiz bir Microsoft aracıdır. IT yöneticileri ve saldırganlar tarafından kullanılır.



Pupy RAT

Açık kaynak kodlu uzaktan komut ve kontrol yazılımı , **APT-35** tarafından Post Exploitation aracı olarak kullanılıyor. Kaynak kodu Python ile yazıldığı için Cross Platform olarak kolayca zararlı üretimi yapılabiliyor. (Windows exe, Python file, PowerShell oneliner/file, Linux elf, APK, Rubber Ducky gibi.)



MITRE ATT&CK Teknikleri

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548):

User Account Control kısa adı (UAC) Windows sistemlerde olan bir güvenlik özelliğidir temel amacı yazılımların İşletim sistemi içine erişimini kısıtlamak veya çalışmasını engellemek . Pupy zararlısı eski sürüm Windows İşletim sistemlerinde UAC bypass yapabilir.

Application Layer Protocol: Web Protocols (T1071):

Zararlı yazılım hedef sistem içinde çalıştığı zaman APT-35 grubuna ait bir komuta kontrol sunucusu ile HTTP üzerinden sürekli olarak iletişim kurar.

Audio Capture (T1123):

Pupy cihaz içinde bulunan mikrofon üzerinden ses kaydı yapabilir.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547):

Pupy zararlısı kendini Registryde “SOFTWARE\Microsoft\Windows\CurrentVersion\Run” içine yükler ve böylece bulaştığı sistem içinde kalıcılık (persistence) özelliği sağlar.

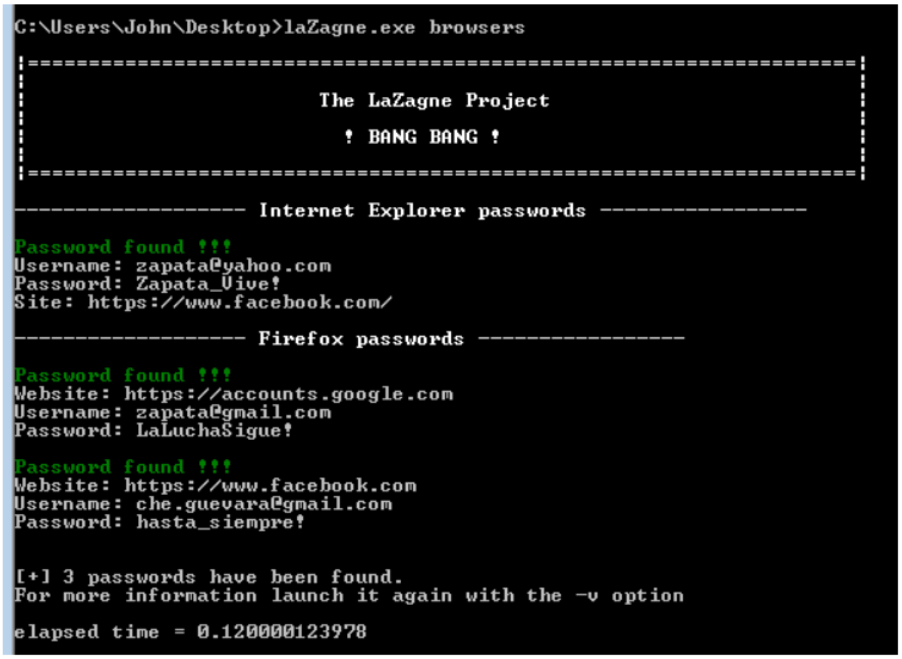
Credentials from Password Stores (T1555) :

Web Browser ve Windows Credentials içinde kayıtlı bulunan şifreleri text formatında alabilir bu işlem için Lazagne isimli açık kaynak kodlu aracı kullanır.

The LaZagne Project !!!

Description

The **LaZagne project** is an open source application used to **retrieve lots of passwords** stored on a local computer. Each software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used software.



This project has been added to pupy as a post-exploitation module. Python code will be interpreted in memory without touching the disk and it works on Windows and Linux host.

Exfiltration Over C2 Channel (T1041):

Hedef cihaz içinden Dosya Çalma (Data Exfiltration) işlemi gerçekleştirir bu veriyi APT-35 grubuna ait server içine yükler.

Input Capture: Keylogging (T1056):

Kullanıcı bilgilerini çalmak için Keylogger özelliğini kullanır.

Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557):

Ağ içinden MITM saldırısı ile kullanıcı şifrelerini veya Browser verilerini çalmayı hedefler.

OS Credential Dumping: LSASS Memory (T1003):

Hedef sistem üzerinden LSASS dump işlemi gerçekleştirip memory içinden Mimikatz aracı ile şifre çalma işlemi gerçekleştirir.

PupyRAT Zararlısı Yayılma Tekniği

Windows Office ile gelen Macro özelliği bir çok zararlı yazılım tarafından kullanılır , Macro ile zararlı yazılım Word,Excel veya PowerPoint formatında genellikle Phishing teknikleri de kullanılıp sistem içinde zararlı yazılım çalıştırır.


وزارة الصحة
Ministry of Health

HealthSecure user registration form

Use this form to apply for a Digital Certificate as an individual user.

If you require assistance completing this form please call NZHSRA (New Zealand Health & Disability Sector Registration Authority) on 0800 117 590.

Click here to complete the form

Please Note: All steps on this application form are mandatory.

New Zealand Health & Disability Sector Registration Authority
In the collection, use and storage of information the NZHSRA will at all times comply with the obligations of the Privacy Act 1993 and the Health Information Privacy Code 1994.

(MD5: 1b5e33e5a244d2d67d7a09c4ccf16e56)

APT35 ilişkili IOC Bilgileri

Hash	Format
43fad2d62bc23ffdc6d301571135222c	MD5 hash
735f5d7ef0c5129f0574bec3cf3d6b06b052744a	SHA1 hash
e5b643cb6ec30d0d0b458e3f2800609f260a5f15c4ac66faf4ebf384f7976df6	SHA256 hash
1b5e33e5a244d2d67d7a09c4ccf16e56	MD5 hash
934c51ff1ea00af2cb3b8465f0a3effcf759d866	SHA1 hash

66d24a529308d8ab7b27ddd43a6 c2db84107b831257efb664044ec4437f9487b	SHA256 hash
03ea9457bf71d51d8109e737158 be888	MD5 hash
d20168c523058c7a82f6d79ef63 ea546c794e57b	SHA1 hash
6c195ea18c05bbf091f09873ed9 cd533ec7c8de7a831b85690e48290b579634b	SHA256 hash
97cb7dc1395918c2f3018c109ab 4ea5b	MD5 hash
3215021976b933ff76ce3436e82 8286e124e2527	SHA1 hash
8d89f53b0a6558d6bb9cdbc9f21 8ef699f3c87dd06bc03dd042290dedc18cb71	SHA256 hash

URL / IP	Format	İçerik
ntg-sa.com	Domain name	Saldırgan tarafından kontrol edilen sahte web sitesi
itworx.com-ho.me	Domain name	Saldırgan tarafından kontrol edilen sahte web sitesi
mci.com-ho.me	Domain name	Saldırgan tarafından kontrol edilen sahte web sitesi
moh.com-ho.me	Domain name	Saldırgan tarafından kontrol edilen sahte web sitesi
mol.com-ho.me	Domain name	Saldırgan tarafından kontrol edilen sahte web sitesi
45.32.186.33	IP address	PupyRAT zararlısını yaymak için kullanılan phishing web sitesi
139.59.46.154	IP Address	PupyRAT zararlısını Powershell ile system içine indirmek için kullanılan web sitesi
89.107.62.39	IP Address	PupyRAT komuta control server.