ISACA
Rome Chapter

APT GROUP MEDIORIENTALI

CHI SONO E COME OPERANO

ANDREA MINGHIGLIONI
THREAT ANALYST

STEFANO MACCAGLIA
MALWARE RESEARCHER

Who we are

Andrea Minghiglioni > Threat Analyst e Incident Responder, opero da anni all'interno dei CSIRT di una nota azienda di Sicurezza italiana. Collaboro regolarmente all'analisi delle nuove minacce e alla gestione di complessi incidenti. Ho partecipato all'analisi di alcuni tra i maggiori incidenti occorsi in Italia negli ultimi anni.

Stefano Maccaglia > Ricercatore e membro del board ISACA italiano, sono anche Advisory Consultant per l'Incident Response di una nota azienda Americana.
Lavoro da anni nella malware analysis e nella threat intelligence.

Who They Are

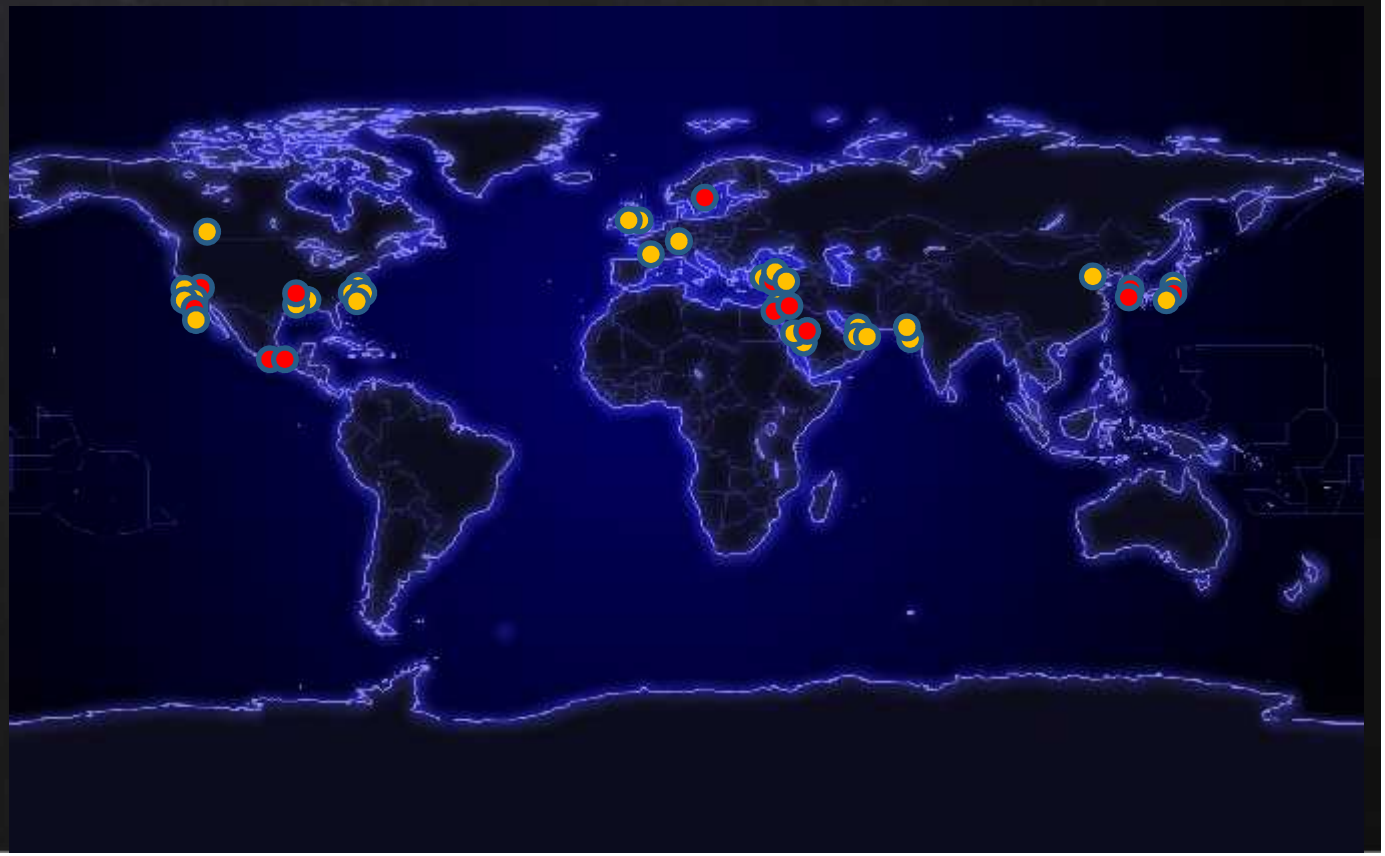
- Si chiamano OpCleaver, Chafer, Cadelle, Shamoon e Rocket Kitten.
- Sono per lo più operativi in Medio Oriente, ma hanno svolto numerose attività maliziose sia di sabotaggio che di cyberspionaggio in Europa e negli USA.
- L'attribuzione della maggior parte è l'Iran e in alcuni casi le attività sono svolte a danno di bersagli coerenti con la politica estera del loro stato di origine.
- Ma perché dovremmo preoccuparci di esaminarli?
- Anzitutto le loro più recenti campagne hanno incluso bersagli europei, in particolare la Francia e la Germania.
- In secondo luogo perché conoscerne le tattiche, le strategie e i tool, permette di anticiparli e di neutralizzarli in modo efficiente.

Il Livello di minaccia di questi attaccanti

- Comparando questi attaccanti ai più famosi APT group russi e cinesi si notano immediatamente alcune differenze.
- Questi attaccanti sono in generale più *"rumorosi"*, ovvero nella prima fase dei loro attacchi usano scansionare in modo sistematico e spesso troppo evidente le vittime.
- Usano più frequentemente le webshell di altri attaccanti.
- Prediligono persistere su macchine Windows.
- Prediligono script Powershell e WMI.
- In alcuni casi riescono a persistere oltre la prima mitigation. (via furto credenziali e uso di at jobs)
- Non hanno tool per la persistenza su macchine Linux-Unix.
- Operano sempre in orari legati all'area medio-orientale.
- Usano domini e server registrati in piccoli provider europei.
- Nel caso di Chafer e Cadelle si sono notati accessi alle macchine infette da indirizzi legati registrati all'Università di Teheran.

OpCleaver

- Il gruppo prende di mira complessi industriali, specialmente del mondo energetico.
- Bersagli preferiti sono gli USA, la Turchia e Israele.
- Gli obiettivi vanno dal sabotaggio al furto di informazioni e brevetti del mondo SCADA.
- In giallo i casi di furto e in rosso quelli di sabotaggio registrati.



OpCleaver: Altri nomi

- ✗ TG-2889 (Threat Group-2889)
- ✗ Cutting Kitten
- ✗ Ghambar
- ✗ Cobalt Gypsy

OpCleaver: Maggiori Operazioni

OPERATION CLEAVER.

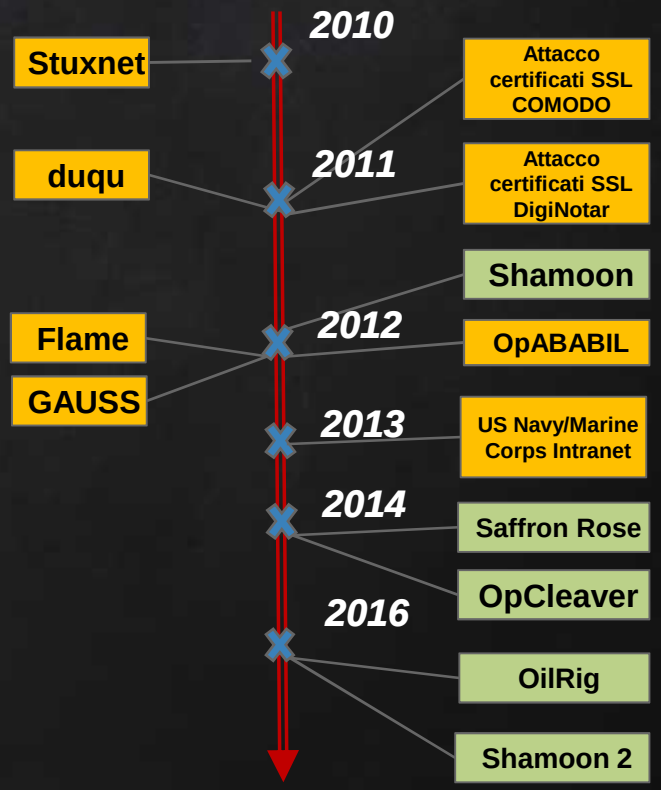
- Si chiama così dal Report di Cylance pubblicato a Dicembre del 2014
- A partire dal 2012 questi attori hanno attaccato ed estratto dati altamente sensibili dai network delle agenzie governative e/o dalle compagnie operanti in settori industriali strategici.

- IL gruppo si caratterizza per l'utilizzo del malware TinyZbot (variante del famigerato trojan Zeus compilata in C#).
- Altri tool usati sono: Mimikatz, PsExec, NetCrawler.

Fonte: https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

OpCleaver: Maggiori Operazioni

- OpCleaver è solo una delle ultime campagne «Iran-centriche»
- A sinistra le operazioni dove l'Iran è stato attribuito come «paese vittima»
- A destra le campagne dove l'Iran è stato attribuito come «paese attaccante»



OpCleaver: Attribuzione

- Numerosi riferimenti (stringhe caratteristiche) all'interno dell'eseguibile più usato dall'attaccante: TinyZBot, come ad esempio:

```
e:\projects\cleaver\trunk\zhoupin_cleaver\obj\x86\release\netscp.pdb
```

- PDB associati al nome dello sviluppatore "Jimbp", come ad esempio:

```
c:\cleaver\binder_1\objusers\jimbp\desktop\binder_1\
```

- PDB associati ad altri artefatti maliziosi come keylogger e infostealer come ad esempio:

```
e:\Projects\Cleaver\trunk\MainModule\obj\Release\MainModule.pdb
```

OpCleaver: Yara Rule

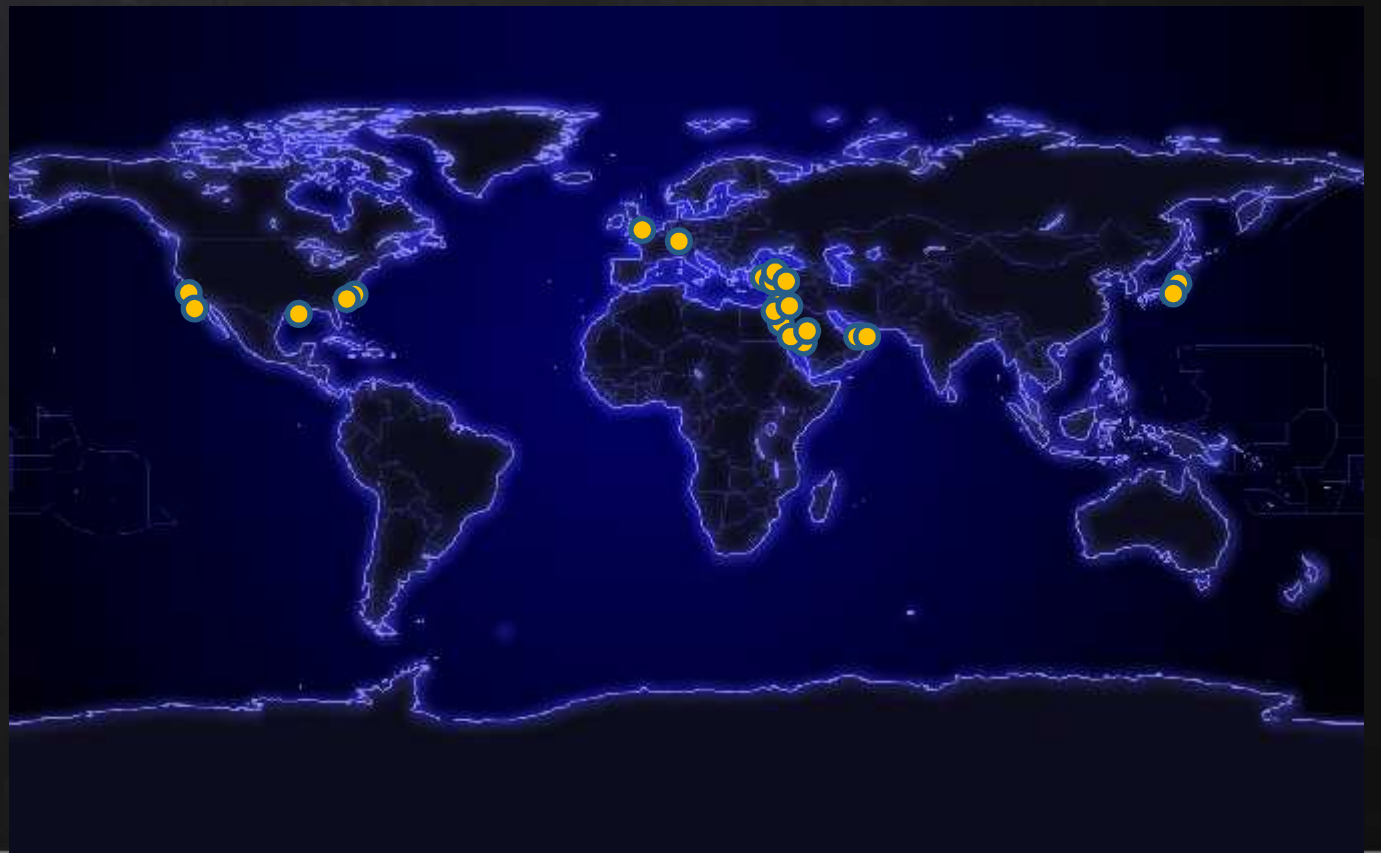
✗ Questa regola è mirata alla rilevazione di TinyZbot:

```
rule tinyzbot {
   strings:
    $s1 = "NetScp" wide
    $s2 = "TinyZBot.Properties.Resources.resources"
    $s3 = "Aoao WaterMark"
    $s4 = "Run_a_exe"
    $s5 = "netscp.exe"
    $s6 = "get_MainModule_WebReference_DefaultWS"
    $s7 = "remove_CheckFileMD5Completed"
    $s8 = "http://tempuri.org/"
    $s9 = "Zhoupin_Cleaver"

  condition:
    ($s1 and $s2) or ($s3 and $s4 and $s5) or ($s6 and $s7 and $s8)
or ($s9)
}
```

Chafer

- Il gruppo svolge operazioni soprattutto a danno di enti strategici come aeroporti, ospedali e ministeri sia dell'area mediorientale che in Asia e in Africa.
- Il gruppo ha mostrato buone capacità tecniche, al punto che oggi è uno dei più problematici tra quelli considerati in questo roundup.



Chafer: Maggiori Operazioni

- Il gruppo ha iniziato a svolgere attività consistenti a partire dal 2011.
- Dal 2015 ha lanciato una massiccia campagna denominata «OilRig»
- I target sono vari, ma sono soprattutto entità governative, dell'area Medio-orientale ed Europea, aeroporti e il settore energetico.
- Il gruppo si caratterizza per l'uso del malware Remexi. Affiancando a questo l'uso di altri tools come:
  - Mimikatz,
  - PSExec
  - Varie WebShell (aspx, php…)
  - Nbtstat
  - plink

Chafer: Attribuzione

- Utilizzo di script VBS attivati da macro in documenti Excel come vettore di infezione iniziale, per scaricare ed installare software aggiuntivo.
- Coincidenza temporale degli attacchi.
- Utilizzo di script Powershell per inviare network beacons alla C&C
- Ricorrenze nelle stringhe usate per il beaconing:

00000000<base 36 of a random number smaller than 46655>.<domainname>.<tld>

- Stessa infrastruttura network (IP) delle C&C dall'analisi degli script Powershell.

Chafer: Yara Rule

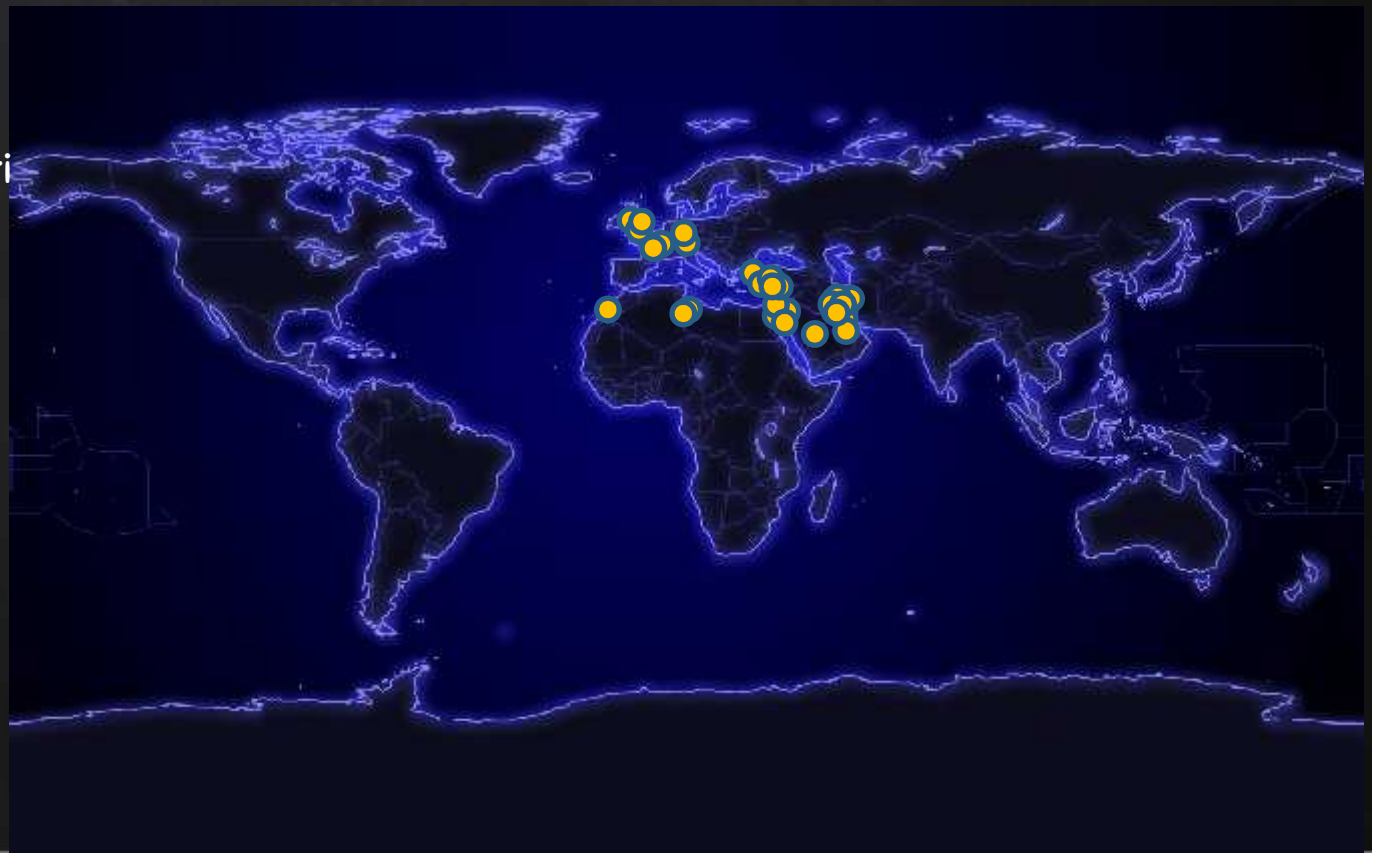
✗ Queste regole sono mirate alla rilevazione di Remexi:

```
rule remexi {
  strings:
    $s01="F:\\95\\95-01\\RCE\\bin\\Release\\x64\\mas.pdb" ascii wide
    $s02="G:\\95-01\\RCE\\bin\\Release\\x64\\mas.pdb" ascii wide
// MZ signature at offset 0 and ...
  condition:
    ($s01 or $s02) and uint16(0) == 0x5A4D and
// ... PE signature at offset stored in MZ header at 0x3C
    uint32(uint32(0x3C)) == 0x00004550
}

rule sea {
  strings:
    $s01="C:\\Users\\Aero\\Documents\\Visual Studio
2015\\Projects\\Sea\\Release\\Sea.pdb" ascii wide
// MZ signature at offset 0 and ...
  condition:
    uint16(0) == 0x5A4D and
// ... PE signature at offset stored in MZ header at 0x3C
    uint32(uint32(0x3C)) == 0x00004550 and all of them
}
```

Cadelle

- Anche questo gruppo prende di mira organizzazioni governative e aziende private dei settori del trasporto e dell'energia.
- I bersagli preferiti si concentrano nell'area del Golfo Persico e nel centro-nord Europa.
- Le attività, nel caso di Cadelle, si concentrano nel furto di informazioni, sopratutto di matrice politica (o geopolitica).
- Alcuni analisti associano questo gruppo a Chafer



Cadelle: Attribuzione

- L'attribuzione di Cadelle è dibattuta.
- Presenta molti tratti in comune con Chafer
- Le timeline degli attacchi molto spesso si sovrappongono.
- Stessi bersagli.
- Una importante differenza è che non condivide la stessa infrastruttura network (IP) per il comando e controllo e per l'accesso ai sistemi vittima.
- Altra significativa differenza è data dall'utilizzo di un malware diverso: Cadelspy.

Cadelle: Yara Rule

✗ Queste regole sono mirate alla rilevazione di Cadelspy

```
rule Cadelle_1
{
 strings:
$s1 = {
56 57 8B F8 8B F1 33 C0 3B F0 74 22 39 44 24 0C
74 18 0F B7 0F 66 3B C8 74 10 66 89 0A 42 42 47
47 4E FF 4C 24 0C 3B F0 75 E2 3B F0 75 07 4A 4A
B8 7A 00 07 80 33 C9 5F 66 89 0A 5E C2 04 00
 }
$s2 = "ntsvc32"
$s3 = "ntbind32"
 condition:
 $s1 and ($s2 or $s3)
}
rule Cadelle_2
{
 strings:
$s1 = "[EXECUTE]" wide ascii
$s2 = "WebCamCapture" wide ascii
$s3 = "</DAY>" wide ascii
$s4 = "</DOCUMENT>" wide ascii
$s5 = "<DOCUMENT>" wide ascii
$s6 = "<DATETIME>" wide ascii
$s7 = "Can't open file for reading :" wide ascii
$s8 = "</DATETIME>" wide ascii
$s9 = "</USERNAME>" wide ascii
$s10 = "JpegFile :" wide ascii
$s12 = "[SCROLL]" wide ascii
$s13 = "<YEAR>" wide ascii
$s14 = "CURRENT DATE" wide ascii
$s15 = "</YEAR>" wide ascii
$s16 = "</MONTH>" wide ascii
$s17 = "<PRINTERNAME>" wide ascii
$s18 = "</DRIVE>" wide ascii
$s19 = "<DATATYPE>" wide ascii
$s20 = "<MACADDRESS>" wide ascii
$s21 = "FlashMemory" wide ascii
 condition:
 12 of them
}
rule Cadelle_3
{
 strings:
$s1 = "SOFTWARE\\ntsvc32\\HDD" wide ascii
$s2 = "SOFTWARE\\ntsvc32\\ROU" wide ascii
 $s3 = "SOFTWARE\\ntsvc32\\HST" wide ascii
 $s4 = "SOFTWARE\\ntsvc32\\FLS" wide ascii
$s5 = "ntsvc32" wide ascii
$s6 = ".Win$py." wide ascii
$s7 = "C:\\users\\" wide ascii
$s8 = "%system32%" wide ascii
$s9 = "\\Local Settings\\Temp" wide ascii
$s10 = "SVWATAUAVAW" wide ascii
$s11 = "\\AppData\\Local" wide ascii
$s12 = "\\AppData" wide ascii
 condition:
 6 of them
}
```

Shamoon e Shamoon 2

- Shamoon, al pari del suo più recente successore (Shamoon2), è principalmente votato al Denial of Service (DoS), ovvero al danneggiamento delle vittime, più che a tentarne il controllo.
- Le azioni più eclatanti di questo gruppo sono state realizzate contro infrastrutture informatiche in vari paesi del mondo, in particolare contro l'Arabia Saudita.

Shamoon e Shamoon 2: Maggiori Operazioni

- Shamoon, noto anche come Disttrack, è un malware modulare scoperto da Symantec, Kaspersky Lab, e Seculert nel 2012.
- Il malware sovrascrive tutti i file del disco di un pc (compreso l'MBR) rendendolo di fatto inutilizzabile e distruggendo tutte le informazioni ivi contenute.
- Nell'ottobre del 2012 un gruppo autodefinitosi «Cutting Sword of Justice» rivendicò la responsabilità per l'attacco verso 35000 workstation appartenenti alla compagnia petrolifera saudita Aramco.
- In Novembre 2016 una nuova campagna è stata lanciata che utilizza un malware simile al precedente (battezzato Shamoon 2 dalla comunità internazionale).
- Tra le più note vittime di Shamoon 2 il Ministero dell'Interno Saudita e la compagnia Sadara Chemical Co.

Shamoon e Shamoon 2: Attribuzione

- Il malware aveva una configurazione di default per iniziare le attività distruttive ad un orario e giorno specifico. (l'inizio del week-end in Arabia Saudita)
- Il malware utilizza 2 componenti principali. Un dropper ed un wiper
- Il dropper crea un servizio (NtsSvr o TrkSvr) per garantirsi persistenza
- Il dropper si diffonde sulla rete attraverso classiche network share smb (Admin$,c$,d$,e$).
- Il wiper cancella un driver esistente sul sistema e lo rimpiazza con un altro driver EldoS' RawDisk driver, un programma legittimo per la cancellazione di file su disco in modo sicuro.
- Il driver è firmato digitalmente ed ha una licenza valida per Agosto 2012
- Il wiper sovrascrive i file con una foto (Aylan)
- Il wiper cambia l'orario del sistema operativo ad Agosto 2012 per rendere utilizzabile la licenza.
- La nuova versione varia dalla precedente di poco: contiene credenziali mirate per un bersaglio diverso dal precedente e alcune variazioni nei nomi dei file e dei domini C&C.

Shamoon: Yara Rule

✗ Questa regola è mirata alla rilevazione di Shamoon

```
rule shamoon
{
 strings:
   $a = "GetPixel" wide ascii
   $b = "CreateCompatibleBitmap" wide ascii
   $c = "CopyMetaFileA" wide ascii
   $d = "iostream stream error" wide ascii
   $e = "\\system32\\" wide ascii
   $f = "GetBrushOrgEx“
   $g = "InitializeCriticalSectionAndSpinCount" wide ascii
   $h = "HOTVGZN#" wide ascii
   $i = "TrkSvr" wide ascii
   $l = "netft429.pnf" wide ascii
   $m = "test456" wide ascii
   $n = "EncodePointer" wide ascii
   $o = "DecodePointer" wide ascii
   $p =
{00C04883C4205BC3CCCCCCCCCCCCCCCC48895C24084889
6C24104889742418574883EC20488B7208498BE8488BFA4885
F67421488B1E488BCEFF15910E000048}
 condition:
   filesize < 2MB and uint16(0) == 0x5A4D and
uint32(uint32(0x3C)) == 0x00004550 and ($p or ( 4 of
($d,$g,$n,$o) and (6 of ($a,$b,$c,$e,$f,$h) or 3 of ($l,$m,$i))))
}
```

Shamoon2: Yara Rule

✗ Queste regole sono mirate alla rilevazione di Shamoon2

```
rule ntertmgr64
{
 strings:
  $a = "GetPixel" wide ascii
  $b = "CreateCompatibleBitmap" wide ascii
  $c = "CopyMetaFileA" wide ascii
  $d = "iostream stream error" wide ascii
  $e = "\\system32\\" wide ascii
  $f = "GetBrushOrgEx“
  $g = "InitializeCriticalSectionAndSpinCount" wide ascii
  $h = "HOTVGZN#" wide ascii
condition:
  uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of them
}
rule vdsk911
{
strings:
  $a = {00 C0 48 83 C4 20 5B C3 CC CC CC CC CC
CCCCCC48895C240848896C24104889742418574883EC20488B7208498BE8488BFA488
5F67421488B1E488BCEFF15910E000048}
condition:
  uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of them
}
```

Rocket Kitten

- Rocket Kitten è il nome dato ad un altro gruppo di origine Iraniana.
- gli obiettivi principali sono aziende e organi governativi in Arabia Saudita,
- Nel mirino c'erano anche ambasciate, diplomatici, addetti militari e personalità di spicco in Afghanistan, Turchia, Qatar, Emirati Arabi Uniti, Iraq, Kuwait e Yemen, oltre ad autorità regionali della Nato.

Rocket Kitten: Maggiori Operazioni

- Le prime identificazioni di Rocket Kitten avvengono da Fire Eye che fa risalire le loro origini al 2010 come «Ajax Security Team»
- Intorno al 2012 gli obbiettivi sembravano limitarsi al solo Iran.
- Tra il 2013 ed il 2014 una serie di campagne denominate come «Rocket Kitten» mostrano un focus maggiore sul cyber-spionaggio.
- Nel 2013 i ricercatori attribuisco a questo gruppo l'operazione «Saffron Rose» consistente in numerosi attacchi ad aziende del settore della difesa degli Stati Uniti.
- Altre operazioni degne di nota sono state: Op Woolen-Goldfish, Oyun e anche l'hack di ID Telegram in Iran del 2016.
- Nel Novembre del 2015 Check Point dichiara di aver identificato uno dei membri del team dietro Rocket Kitten nella persona di Yaser Balaghi, aka Wool3n.H4t.

https://www.scmagazine.com/check-point-publishes-report-on-rocket-kitten-techniques/article/533439/

Rocket Kitten: Attribuzione

- Riferimenti in Farsi all'interno del codice analizzato.
- Utilizzo di numerosi tool tra cui spicca GHOLE, una versione modificata del tool di PT Core Impact.
- Altri tool caratteristici: CWoolger, FireMalv, .NETWoolger, MPK, Puppy RAT, MagicHound.Leash (IRC Bot)
- Uso di tool open source

Rocket Kitten: Yara Rule

✗ Queste regole sono mirate alla rilevazione di Rocket Kitten

```
rule RocketKitten_Keylogger {
   strings:
      $x1 = "\\Release\\CWoolger.pdb" ascii
      $x2 = "WoolenLoger\\obj\\x86\\Release" ascii
      $x3 = "D:\\Yaser Logers\\"
      $z1 = "woolger" fullword wide
      $s1 = "oShellLink.TargetPath = \"" fullword ascii
      $s2 = "wscript.exe " fullword ascii
      $s3 = "strSTUP = WshShell.SpecialFolders(\"Startup\")" fullword ascii
      $s4 = "[CapsLock]" fullword ascii
   condition:
/* File detection */
      (uint16(0) == 0x5a4d and filesize < 200KB and (1 of ($x*) or ($z1 and 2 of ($s*)))) or
/* Memory detection */
      ($z1 and all of ($s*))
}
```


Q&A