INCIDENT RESPONSE INSIGHTS

OCTOBER 2024

BASED ON INCIDENT DATA AS OF END OF SEPTEMBER 2024

Disclaimer: The content of this document is for informational purposes only. Booz Allen Hamilton is not responsible for your reliance on, or implementation of the guidance described in this document.

Booz
Allen

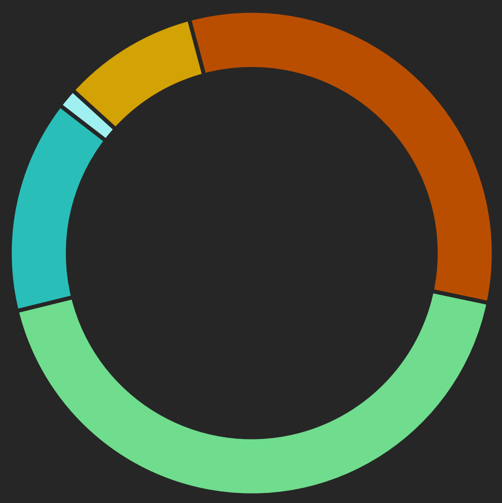
Booz Allen.

Monthly Incident Metrics

In September, we saw an increase in Email Compromise and other types of matters (such as Insider Threat and General Malware) but did see a decline in Ransomware and Network Intrusion matters compared to the previous month.

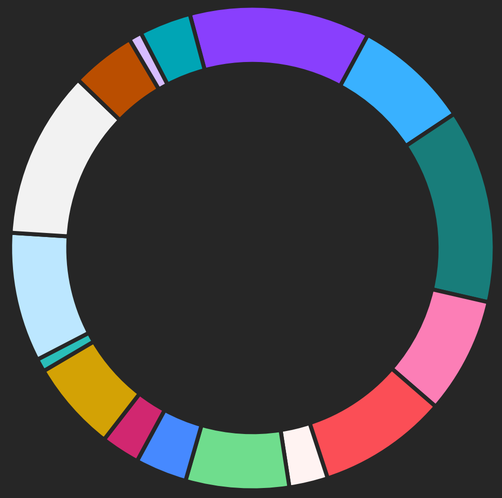
We saw a marked increase in matters across many industry sectors including Manufacturing, Construction, Legal, Healthcare, Financial Services, Consulting and Transportation, but a decline in matters across Real Estate, Government and Energy sectors compared to the previous month. Matters across Technology / Communications clients were about the same as last month.

Incidents by Types – September 2024



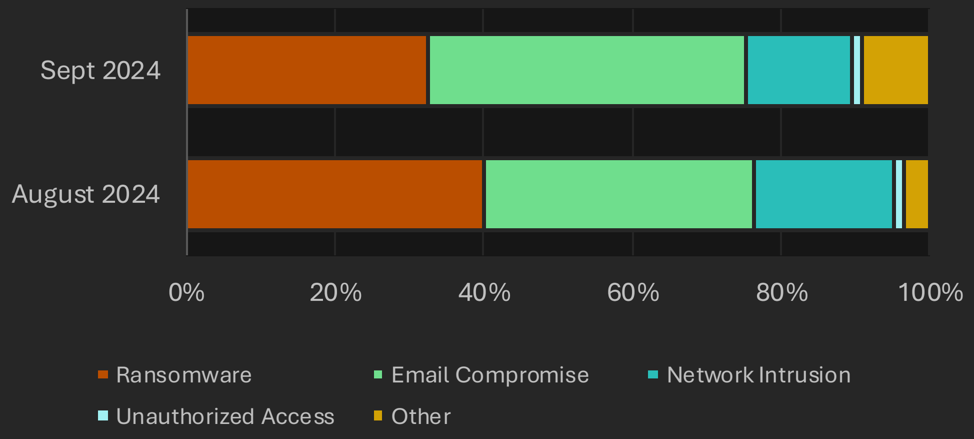
Ransomware	32%	↓ -26%
Email Compromise	43%	↑ 6%
Network Intrusion	14%	↓ -31%
Unauthorized Access	1%	NA
Other	9%	↑ 133%

Incidents by Industry – September 2024

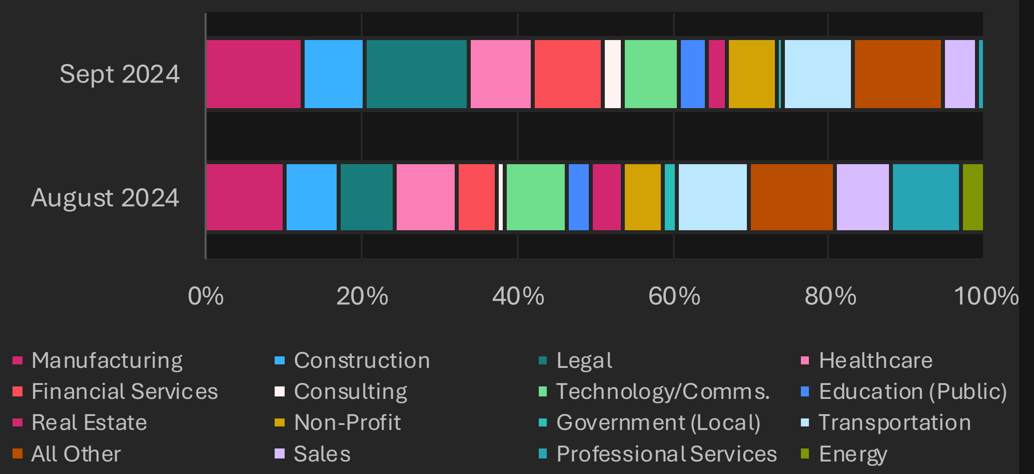


Manufacturing	12%	↑ 40%
Construction	8%	↑ 29%
Legal	13%	↑ 114%
Healthcare	8%	↑ 13%
Financial Services	9%	↑ 100%
Consulting	3%	↑ 200%
Technology/Comms.	7%	NA
Education (Public)	3%	↑ 33%
Real Estate	3%	↓ -25%
Non-Profit	6%	↑ 40%
Government (Local)	1%	↓ -50%
Transportation	9%	↑ 11%
All Other	11%	↑ 18%
Energy	0%	↓ -100%

Incidents Types Monthly Trends



Incidents Industry Monthly Trends

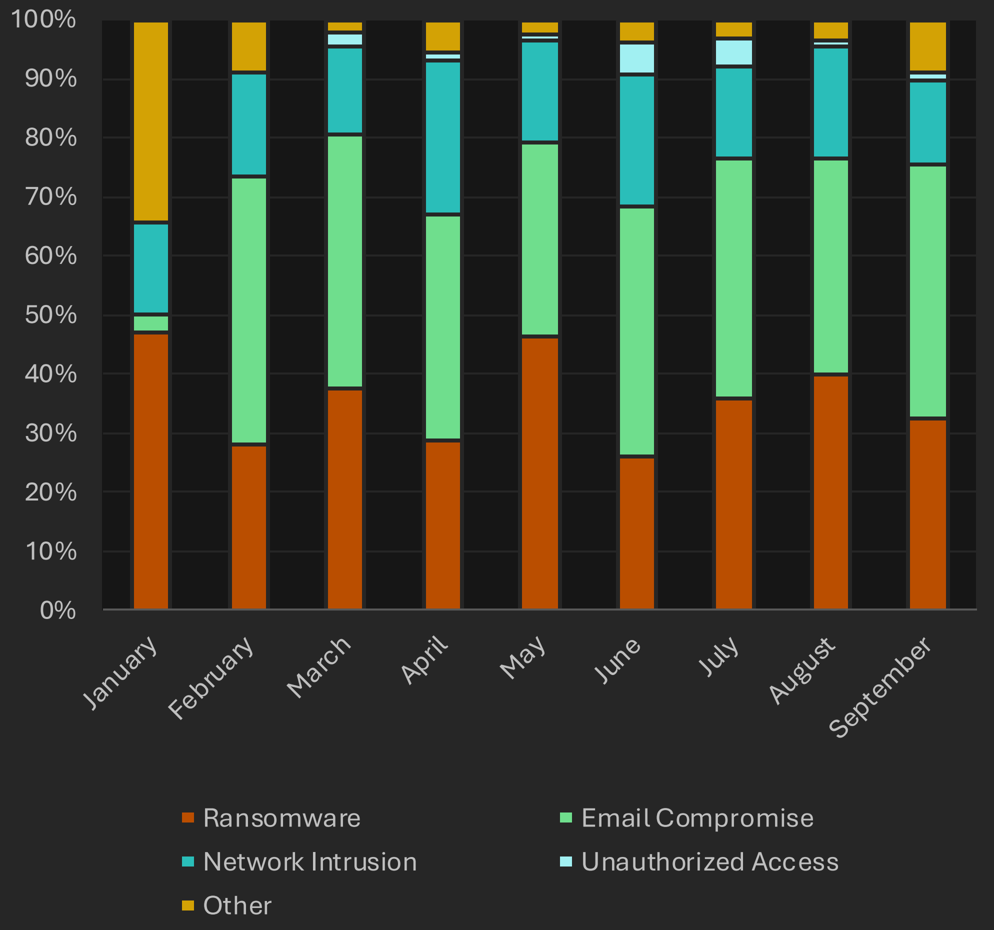


Incident YTD Trends

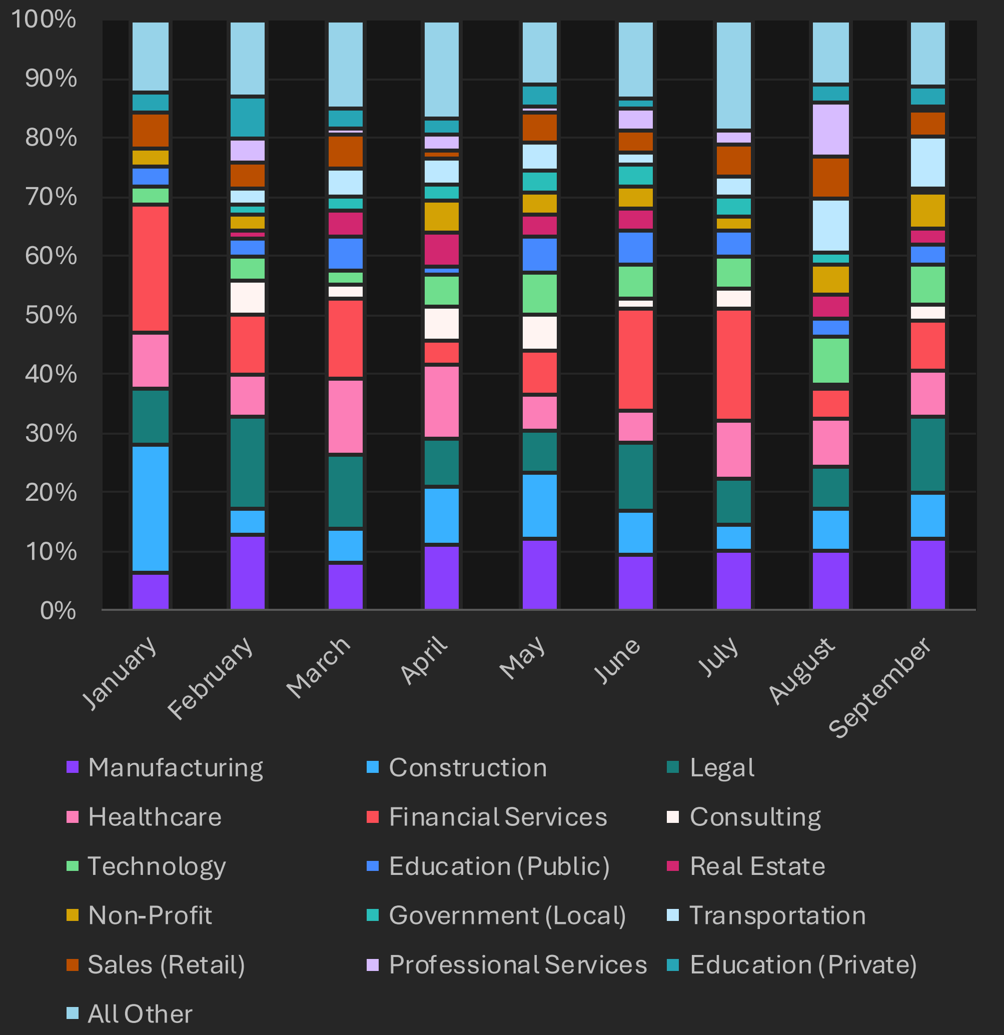
For the year so far, Ransomware matters have dominated our case load and have been between ~30% to ~50% of the total incident volume, followed by Email Compromise making up ~10% to ~40% of the total incident volume. For Q3 2024, we saw a continued increase in Ransomware, Email Compromise and Network Intrusion matters.

The top five most impacted sectors are consistently across Manufacturing, Financial Services, Construction, Healthcare and Legal organizations, making up between ~50% to ~70% of our caseload each month. For Q3 2024, we saw a broad array of industries being targeted by threat actors.

Incidents by Types – 2024 YTD



Incidents by Industry – 2024 YTD



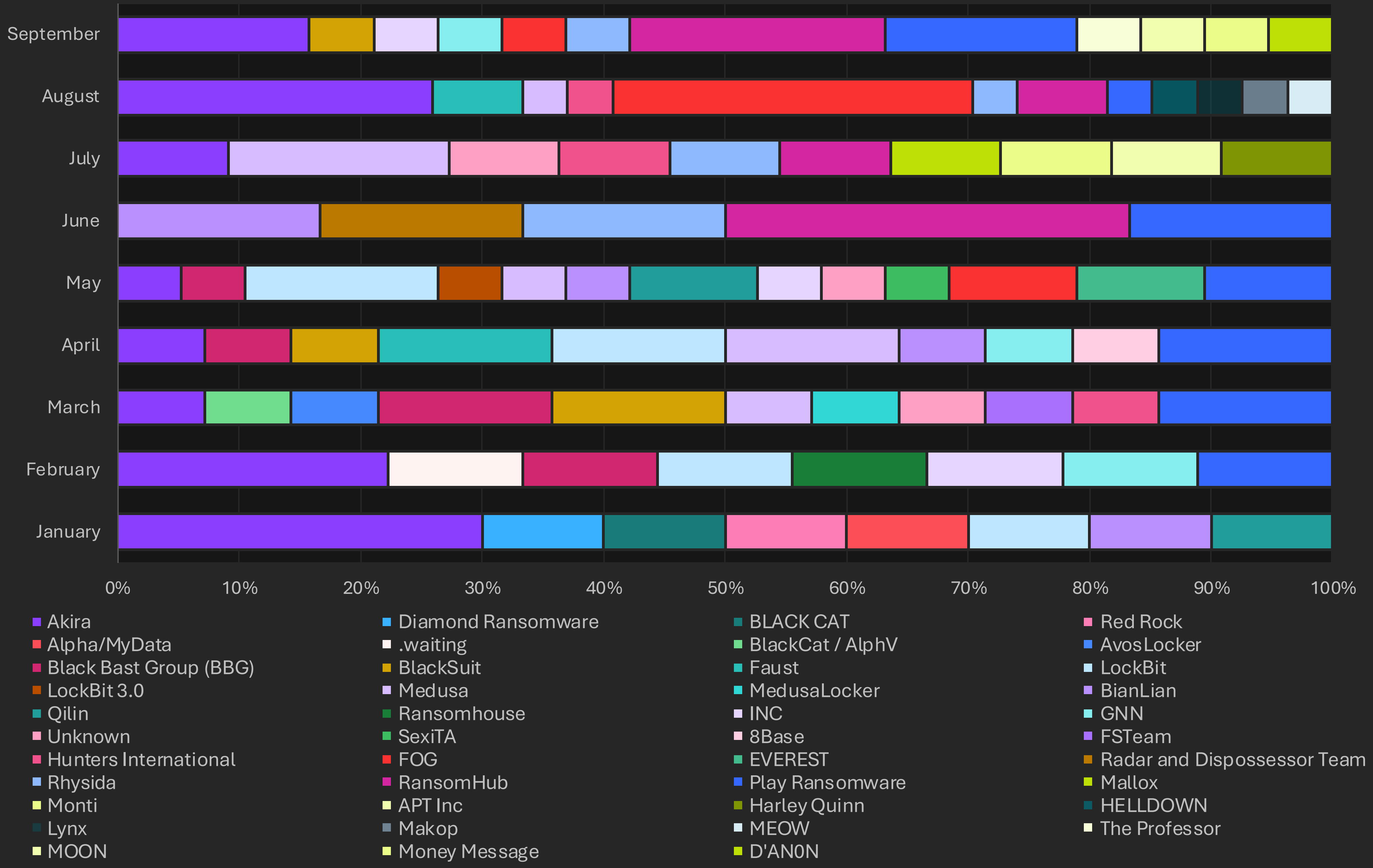
Booz Allen®

Threat Actor YTD Trends

In Q3 2024, we observed Play Ransomware Group, Akira, FOG, RansomHub, Rhysida, Blacksuit and GNN Threat Actor Groups dominating the Ransomware landscape.

Additionally, in Q3 2024, we observed a few new Threat Actor groups such as MOON, Money Message, D’An0n, Helldown, Makop, Meow and Lynx impacting our clients.

Threat Actors 2024 YTD



Booz
Allen

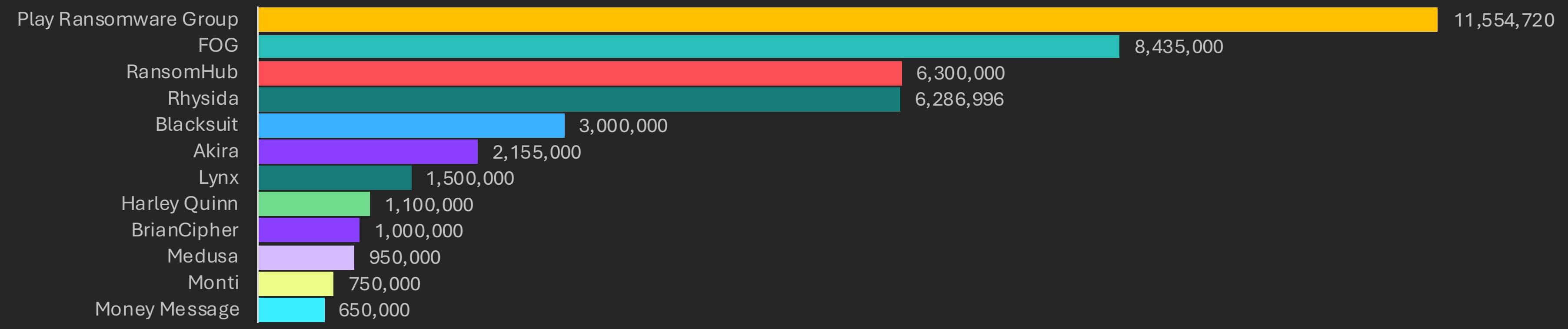
Ransom Demand By Threat Actors

For Q1 2024, Play Ransomware Group, Lockbit, Akira and Ransomhouse led on ransom demands.

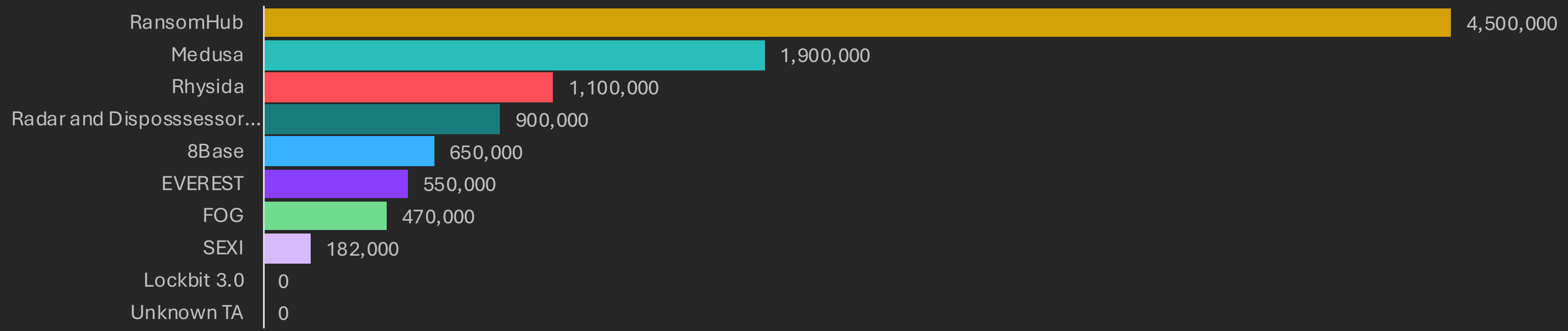
In Q2 2024, RansomHub, Medusa, Rhysida, and Radar and Dispossessor Team led on ransom demands.

In Q3 2024, Play Ransomware Group, FOG, RansomHub, Rhysida, Blacksuit and Akira have led on ransom demands.

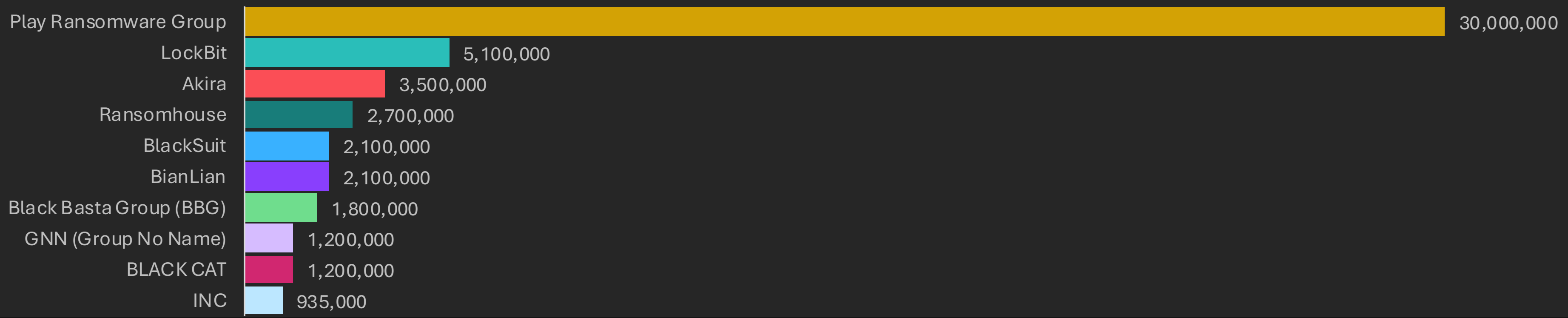
2024 Q3 (July, August, September)



2024 Q2 (April, May, June)



2024 Q1 (January, February, March)



IR Update Summary

Read on for a summary of our Incident Response team's recent observations alongside insights from across the cybersecurity community. The information shared here is intended to provide a snapshot of current activity and is subject to change as the various threat group tactics, techniques, and procedures evolve.

Highlights

- *Akira Ransomware Update*
- *New Ransomware Groups with Unique Business Models*
- *Partner Update: Cloudflare: Multi-Channel Phishing*

Akira Ransomware Update

Booz Allen has recently detected notable dysfunction within the Akira ransomware group. In recent weeks, Akira's operations have become increasingly disorderly, marked by persistent technical problems such as chat portal outages and failed message transmissions. Affiliate behavior has also been inconsistent, with some affiliates being unresponsive while others are unusually aggressive and impulsive. Furthermore, there has been a noticeable decline in demand for their services and exfiltration activities. Several months ago, Akira frequently failed to exfiltrate client data, suggesting internal disruptions. This suspicion was further supported by the appearance of a spin-off group, PowerRangers, which utilized Akira's leak site and chat rooms but employed a different encryption extension. These patterns of internal strife, technical challenges, and erratic affiliate actions echo the period when the government initially seized LockBit. Booz Allen will continue to closely monitor the situation to effectively understand and address these developments.

Booz Allen has recently noted significant issues within the Akira ransomware group. Akira's operations have become increasingly chaotic, with frequent technical problems like chat portal outages and failed message transmissions. Affiliate behavior has been erratic, varying from unresponsive to unusually aggressive. Demand and exfiltration activities have also decreased. Previously, Akira often failed to exfiltrate client data, suggesting internal disruptions. This suspicion grew with the rise of a spin-off group, PowerRangers, which used Akira's leak site and chat rooms but with a different encryption extension. These patterns are similar to those seen when the government initially seized LockBit. Booz Allen will continue to monitor these developments closely.

New Ransomware Groups with Unique Business Models

Booz Allen recently identified a new threat actor group called HellDown. The distinctive feature of this group is their immediate disclosure of victim companies on their leak site, and they won't remove these announcements without payment. Interestingly, the URL for HellDown's leak site starts with "Onyx," which is another ransomware group, though any connection between the two groups remains unclear. Research into Onyx shows that their encryptor destroys all files larger than 2 MB instead of encrypting them and buying the decrypter doesn't resolve the errors. Moreover, it appears that Onyx does not provide the decrypter even after payment. The Booz Allen TACI team has yet to encounter Onyx directly but continues to study their tactics.

Another group, similar to HellDown in their business model, is Meow. This group also immediately discloses their victims on their leak site. However, instead of offering victim data for free download, they provide two pricing options: one higher price for a one-time payment and deletion of the data, and a lower price for purchasing the data without deletion, allowing the group to resell it multiple times. During interactions with Booz Allen, this group refused to remove postings without payment and admitted to selling the data numerous times. Given this situation, paying a ransom to suppress victim data is not recommended because it is likely already accessible to multiple unknown parties. Notably, the Hello Kitty icon appears on the browser tab when viewing this group's leak site. Whether there is any relationship between Meow and the Hello Kitty brand or if this is just coincidental is unknown, but the Booz Allen TACI team will continue to observe the situation

Updates from our Partners: Cloudflare: Multi-Channel Phishing Update

Recently, Cloudflare has seen an increase in multi-channel and phased phishing, where several unique methods and technologies are used to send malicious links, files, and elicit compromises. Some of the most common channels used in these phased schemes include SMS (text messaging) and public and private messaging applications. Bad actors are increasingly leveraging attack vectors that take advantage of the tools people use every day to consume information and work. Cloud collaboration tools, such as Google Workspace, Atlassian, and Microsoft Office, are often used to emulate legitimate requests for document sharing and information. However, attackers are leveraging these channels to receive and exchange links and files alongside email phishing endeavors. A common scenario is a seemingly legitimate request for a document or file share that is sent to the target via email. Then, the target recipient is asked to upload the desired information to a compromised cloud collaborative folder or tool. In addition to email phishing, web and social phishing have also been on the rise, targeting people on LinkedIn and X (formerly Twitter). As these schemes increase in sophistication, they become more difficult to combat using traditional security software and prevention measures. To protect against these different vectors, organizations must educate their employees on differing phishing schemes and social engineering so that they are more aware of what a threat can look like – and to think before they click, respond, or react. IT and security teams must also remain current on the latest vectors used in multi-channel phishing efforts to better defend their organizations against these complex attacks.

IR Update Summary (cont.)

Read on for a summary of our Incident Response team’s recent observations alongside insights from across the cybersecurity community. The information shared here is intended to provide a snapshot of current activity and is subject to change as the various threat group tactics, techniques, and procedures evolve.

Highlights

- *New Google Workspace Feature : Context-Aware Access*
- *New SonicWall SSL Vulnerability*

New Google Workspace Feature: Context-Aware Access

Google Workspace has implemented a new feature: "Context-Aware Access." This feature is similar to Microsoft's conditional access policies, giving the administrators control over which applications a user can access based on context, such as device security status, location, and IP address. Organizations can use this feature to allow access to applications only from within the corporate network or from company-issued devices. Administrators can even restrict applications such as Google Drive so that a user can only access Google Drive if their storage device is encrypted. With these Context-Aware Access policies, organizations can better secure access to their Google Workspace environment and data.

There are some restrictions to the Context-Aware Access feature from Google Workspace. To use the feature, the environment must have a supported edition. Supported editions include Frontline Standard, Enterprise Standard and Enterprise Plus, Education Standard and Education Plus, Enterprise Essentials Plus, or Cloud Identity Premium. Users must be super admins or delegated admins with the following privileges to create a Context-Aware Access policy: DataSecurity with Access level management and Rule management, as well as Admin API Privileges with Groups Read and Users Read. You cannot enforce Context-Aware Access policies for third-party native applications such as Spotify on mobile devices. However, you can enforce Context-Aware Access policies on Security Assertion Markup Language (SAML) applications on mobile devices accessed using the Chrome web browser.

You can implement Context-Aware Access policies for web and native applications on desktop and mobile applications. After granting access, the program continuously evaluates access, except for SAML applications, which it only evaluates upon sign-in. For example, if a user signs into a SAML application at the office and then walks out of the building to lunch, the user keeps access to the application despite changing location. The Context-Aware Access policy only gets rechecked whenever a session ends, and the user has to reauthenticate for SAML applications.

Before deploying a new Context-Aware Access policy, administrators can test the policy using what Google Workspace refers to as "monitor mode." This mode lets the administrator simulate the impact of enforcing an access policy without blocking user access

Google Workspace Feature (contd.)

. Google Workspace recommends deploying a new access policy in monitor mode for at least a week and monitoring the events logged within the Context-Aware Access log to show which users would be blocked if the access policy were in place. Once the administrator verifies that the access policy is working for the intended purpose, they can move it to "active mode," which will enforce the policy within the Google Workspace environment.

References:
https://support.google.com/a/answer/12645308?hl=en&ref_topic=9262521&sjid=5705994952188872445-NC

New SonicWall SSL Vulnerability

Booz Allen has seen the usage of client VPN devices as the entry point for several recent incidents. This trend is understandable, given the many vulnerabilities discovered on these devices. On August 22, 2024, SonicWall published CVE-2024-40766 with a severity rating of 9.3. The CVE surrounds an improper access control vulnerability in the SonicWall SonicOS management interface and the SSLVPN feature. Successful exploitation of the vulnerability allows a remote, unauthenticated attacker to gain unauthorized access to resources and cause the firewall to crash. The CVE is known to affect SonicWall Firewall Generation 5, 6, and 7 devices running SonicOS versions 7.0.1-5035 and older. SonicWall has patched the vulnerability, and clients are encouraged to update the program as soon as possible. Booz Allen believes that the CVE affects devices whose user accounts are local to the device without enabling multi-factor authentication (MFA). The US Cybersecurity and Infrastructure Security Agency (CISA) has added the CVE to its Known Exploited Vulnerabilities catalog, indicating that exploitation of this CVE is occurring in the wild.

Mitigation Strategies:

1. Update vulnerable SonicOS versions with the latest patched version.
2. Enable MFA on all SSLVPN accounts.
3. Update all local device user passwords to enhance security and prevent unauthorized access.

References: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

Booz Allen

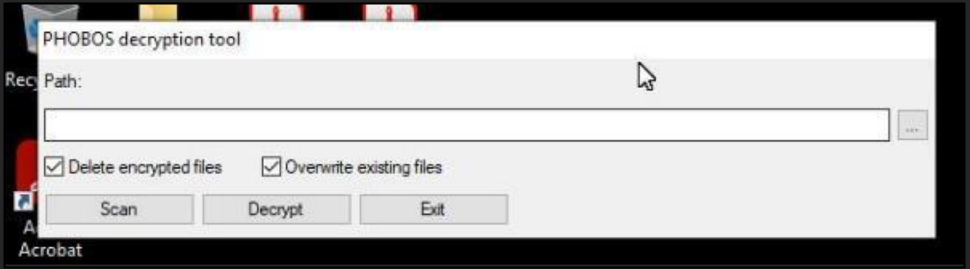
Malware Analysis Insights

Read on for a summary of analysis performed by our Reverse Malware Engineering (RME) team of a Decrypter tool received by a client, that was found to contain mechanisms for persistence, lateral movement, keystroke monitoring, command & control and possible re-infection.

Threat Actor Decrypter Tool Reverse Engineering Analysis

Booz Allen's Reverse Malware Engineering team received a request to analyze a scan tool/decryption tool for suspicious activities. The threat actor supplied two files: a RAR archive and a text document. The text document included the password needed to extract the RAR archive as well as additional instructions the victim should follow. The archive contained an EXE file that appears to be similar to scan tools used in previous incidents, but indications point to it being compromised with the XRed malware strain..

- File_01 Findings (ph_decrypt.rar): The RAR archive, ph_decrypt.rar, was confirmed to be a standard password-protected RAR file containing the malicious executable ph_decrypt.exe. The password for the archive was provided in the accompanying text file.
- File_02 Findings (ph_decrypt.exe): The executable file ph_decrypt.exe was identified as malicious, performing various harmful activities such as dropping additional malicious files, installing persistence mechanisms, and communicating with known malicious IP addresses. It was categorized under the XRed malware family.
- Trojanized Nature: The executable file displayed a graphical user interface similar to legitimate scanning tools (Figure 1) but exhibited malicious behavior, indicating it was trojanized for potential re-exploitation. The file copies itself to “C:\ProgramData\Synaptics\Synaptics.exe” as seen from a hash comparison (Figure 2) and altered system registry keys for persistence (Figure 3).
- Persistence Mechanism: The malware maintained its presence on the system by creating and modifying registry keys (Figure 3), performing a mutex check, and attempting to download additional payloads from pre-programmed URLs (Figure 4). It also collected system information and sent it to the attacker via SMTP.

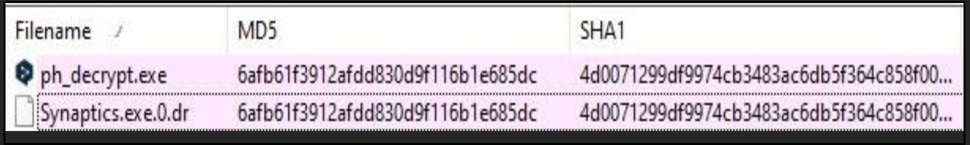


PHOBOS decryption tool

Path:

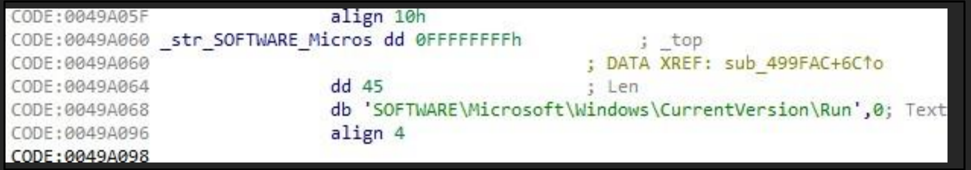
☑ Delete encrypted files ☑ Overwrite existing files

Figure 1: Scan Tool GUI



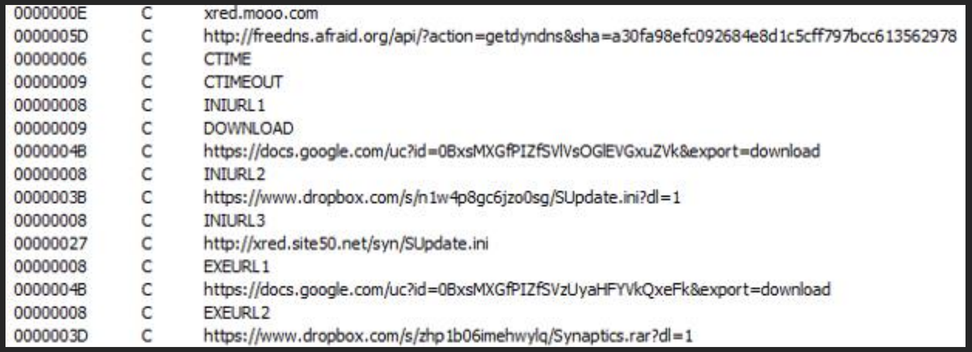
Filename	MD5	SHA1
ph_decrypt.exe	6afb61f3912afdd830d9f116b1e685dc	4d0071299df9974cb3483ac6db5f364c858f00...
Synaptics.exe.0.dr	6afb61f3912afdd830d9f116b1e685dc	4d0071299df9974cb3483ac6db5f364c858f00...

Figure 2: Hash Comparison of Copied Files



```
CODE:0049A05F                  align 10h
CODE:0049A060 _str_SOFTWARE_Micros dd 0FFFFFFFFh          ; _top
CODE:0049A060                                         ; DATA XREF: sub_499FAC+6C↑o
CODE:0049A064                  dd 45                  ; Len
CODE:0049A068                  db 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run',0; Text
CODE:0049A096                  align 4
CODE:0049A098
```

Figure 3: Startup Registry Key for Persistence



```
0000000E    C    xred.mooo.com
0000005D    C    http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978
00000006    C    CTIME
00000009    C    CTIMEOUT
00000008    C    INIURL1
00000009    C    DOWNLOAD
0000004B    C    https://docs.google.com/uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download
00000008    C    INIURL2
0000003B    C    https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1
00000008    C    INIURL3
00000027    C    http://xred.site50.net/syn/SUpdate.ini
00000008    C    EXEURL1
0000004B    C    https://docs.google.com/uc?id=0BxsMXGfPIZfSVzUyaHFYVkQxeFk&export=download
00000008    C    EXEURL2
0000003D    C    https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1
```

Figure 4: URLs and Email Strings found in the Binary

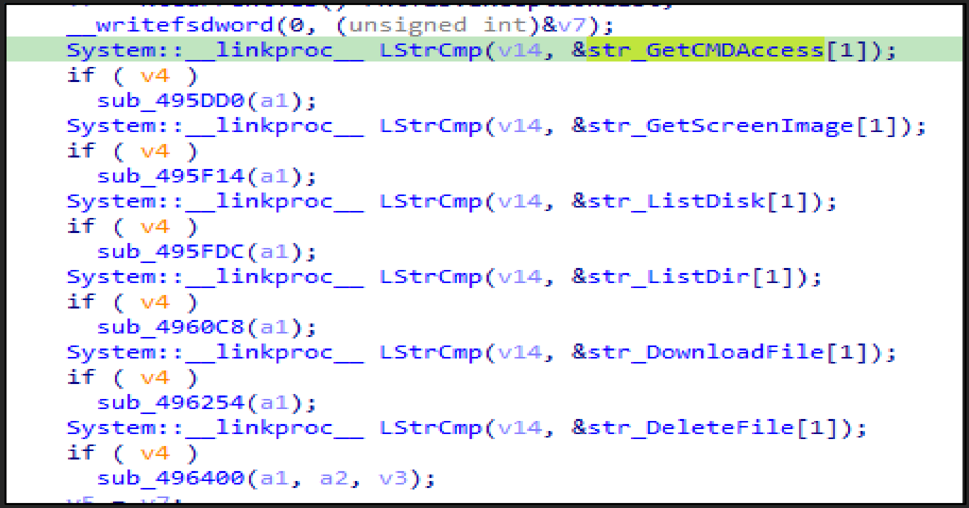
Malware Analysis Insights (cont.)

Read on for a summary of analysis performed by our Reverse Malware Engineering (RME) team of a Decrypter tool received by a client, that was found to contain mechanisms for persistence, lateral movement, keystroke monitoring, command & control and possible re-infection.

Threat Actor Decrypter Tool Reverse Engineering Analysis (contd.)

- Keystroke Logging: The malware included keylogging capabilities through keyboard hooking and key mappings, allowing it to monitor and record keystrokes.
- Remote Commands: The malware allowed remote command execution by an attacker's server (Figure 5), enabling actions such as obtaining command prompt access, capturing screenshots, listing disks and directories, downloading and deleting files.
  - GetCMDAccess – obtain command prompt access
  - GetScreenImage – capture screenshot
  - ListDisk – list disks
  - ListDir – list directories
  - DownloadFile – download file
  - DeleteFile – delete file
- USB Propagation Capability: The malware had the ability to propagate via USB drives by generating an autorun.inf file if it did not already exist on the inserted drive (Figure 6).
- Lastly, the malware includes a secured VBA script embedded within it, which duplicates an XLSM file that is already present on the disk and inserts malicious VBA code into it. The script then alters the registry settings to suppress security alerts for VBA macros (Figure 7).

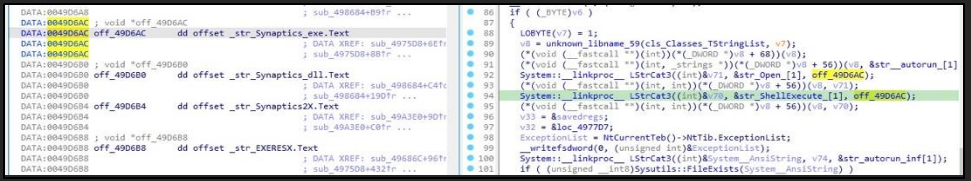
As evident from our analysis, this particular decrypter/malware possesses various functions such as maintaining presence on a system, executing commands remotely, data theft, spreading through USB devices, and monitoring keystrokes. It is imperative that a thorough analysis of any tool provided by the TA or obtained by other means, be conducted to prevent persistence and re-infection.



```
__writefsdword(0, (unsigned int)&v7);
System::__linkproc__ LStrCmp(v14, &str_GetCMDAccess[1]);
if ( v4 )
  sub_495DD0(a1);
System::__linkproc__ LStrCmp(v14, &str_GetScreenImage[1]);
if ( v4 )
  sub_495F14(a1);
System::__linkproc__ LStrCmp(v14, &str_ListDisk[1]);
if ( v4 )
  sub_495FDC(a1);
System::__linkproc__ LStrCmp(v14, &str_ListDir[1]);
if ( v4 )
  sub_4960C8(a1);
System::__linkproc__ LStrCmp(v14, &str_DownloadFile[1]);
if ( v4 )
  sub_496254(a1);
System::__linkproc__ LStrCmp(v14, &str_DeleteFile[1]);
if ( v4 )
  sub_496400(a1, a2, v3);
```

Figure 5: Remote Commands

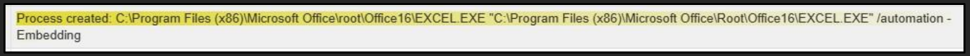
```
[autorun]
open=Synaptics.exe
shellexecute=Synaptics.exe
```



```
DATA:0049D6A8                                           ; sub_498684+B9↑r ...
DATA:0049D6AC ; void *off_49D6AC
DATA:0049D6AC off_49D6AC      dd offset _str_Synaptics_exe.Text
DATA:0049D6AC                                           ; DATA XREF: sub_4975D8+6E↑r
DATA:0049D6AC                                           ; sub_4975D8+8B↑r ...
DATA:0049D6B0 ; void *off_49D6B0
DATA:0049D6B0 off_49D6B0      dd offset _str_Synaptics_dll.Text
DATA:0049D6B0                                           ; DATA XREF: sub_498684+C4↑c
DATA:0049D6B0                                           ; sub_498684+19D↑r ...
DATA:0049D6B4 off_49D6B4      dd offset _str_Synaptics2X.Text
DATA:0049D6B4                                           ; DATA XREF: sub_49A3E0+9D↑r
DATA:0049D6B4                                           ; sub_49A3E0+C0↑r ...
DATA:0049D6B8 ; void *off_49D6B8
DATA:0049D6B8 off_49D6B8      dd offset _str_EXERESX.Text
DATA:0049D6B8                                           ; DATA XREF: sub_49686C+96↑r
DATA:0049D6B8                                           ; sub_4975D8+432↑r ...
```

```
if ( (_BYTE)v6 )
{
  LOBYTE(v7) = 1;
  v8 = unknown_libname_59(cls_Classes_TStringList, v7);
  (*(void (__fastcall **)(int))(*(_DWORD *)v8 + 68))(v8);
  (*(void (__fastcall **)(int, _strings *))(*(_DWORD *)v8 + 56))(v8, &str__autorun_[1]
  System::__linkproc__ LStrCat3((int)&v71, &str_Open_[1], off_49D6AC);
  (*(void (__fastcall **)(int, int))(*(_DWORD *)v8 + 56))(v8, v71);
  System::__linkproc__ LStrCat3((int)&v70, &str_ShellExecute_[1], off_49D6AC);
  (*(void (__fastcall **)(int, int))(*(_DWORD *)v8 + 56))(v8, v70);
  v33 = &savedregs;
  v32 = &loc_4977D7;
  ExceptionList = NtCurrentTeb()->NtTib.ExceptionList;
  __writefsdword(0, (unsigned int)&ExceptionList);
  System::__linkproc__ LStrCat3((int)&System__AnsiString, v74, &str_autorun_inf[1]);
  if ( (unsigned __int8)Sysutils::FileExists(System__AnsiString) )
```

Figure 6: Autorun Capability



```
Process created: C:\Program Files (x86)\Microsoft Office\root\Office16\EXCEL.EXE "C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" /automation -
Embedding
```

Figure 7: Excel Process Initiated

Booz
Allen®

INCIDENT RESPONSE CONTACT DETAILS

Email: incident@bah.com
U.S. Hotline: +1 (888) 266-9478 “BOOZ-IRT”
UK/EU Hotline: +44 (808) 296-8080

Brendan Rooney
Senior Vice President
Global Incident Response

Tony Gaidhane
Vice President
Global Incident Response