# MITRE ATT&CK®
# Matrix Introspection

baesystems.com/cyber

An evolution in identifying and tracking cyber attackers

BAE SYSTEMS

# Background

It's a common belief in the security industry that new attacks involve new techniques, e.g. new vulnerabilities being exploited or new tricks for lateral movement. From our perspective, the vast majority of attacks leverage existing and often well-known techniques and are only successful because of poor implementation of controls or gaps in detection. Therefore a better articulation of these known techniques, as well as adoption of machine-readable intelligence formats should both improve security coverage for organisations and reduce the burden on network defenders.

The leading initiative in tackling this is the **MITRE ATT&CK® Matrix** for categorising and describing threat actor techniques, which has continued to evolve and increase in popularity. Many teams are now using it routinely for threat modelling, security testing, and other use cases. Many vendors of security products now include some level of linkage to the ATT&CK matrix.

We recently ran an exercise to review our back catalogue of threat research reports over the past six years. Given the volume of content, this required automatic extraction by pattern matching followed by manual validation from our analyst team. This analysis was performed against the ATT&CK Matrix v6. There have been a number of changes made to the ATT&CK Matrix since this time, which we discuss later in the report.

This report provides a summary of our findings as well as recommendations on how to make use of the MITRE ATT&CK Matrix.

# Analysis

Over the past six years we have produced **over 500 detailed research reports** based on cases from our incident response team and threat intel investigations.

As marked on the below graph, different ATT&CK tactics vary considerably in their total coverage in our reports:

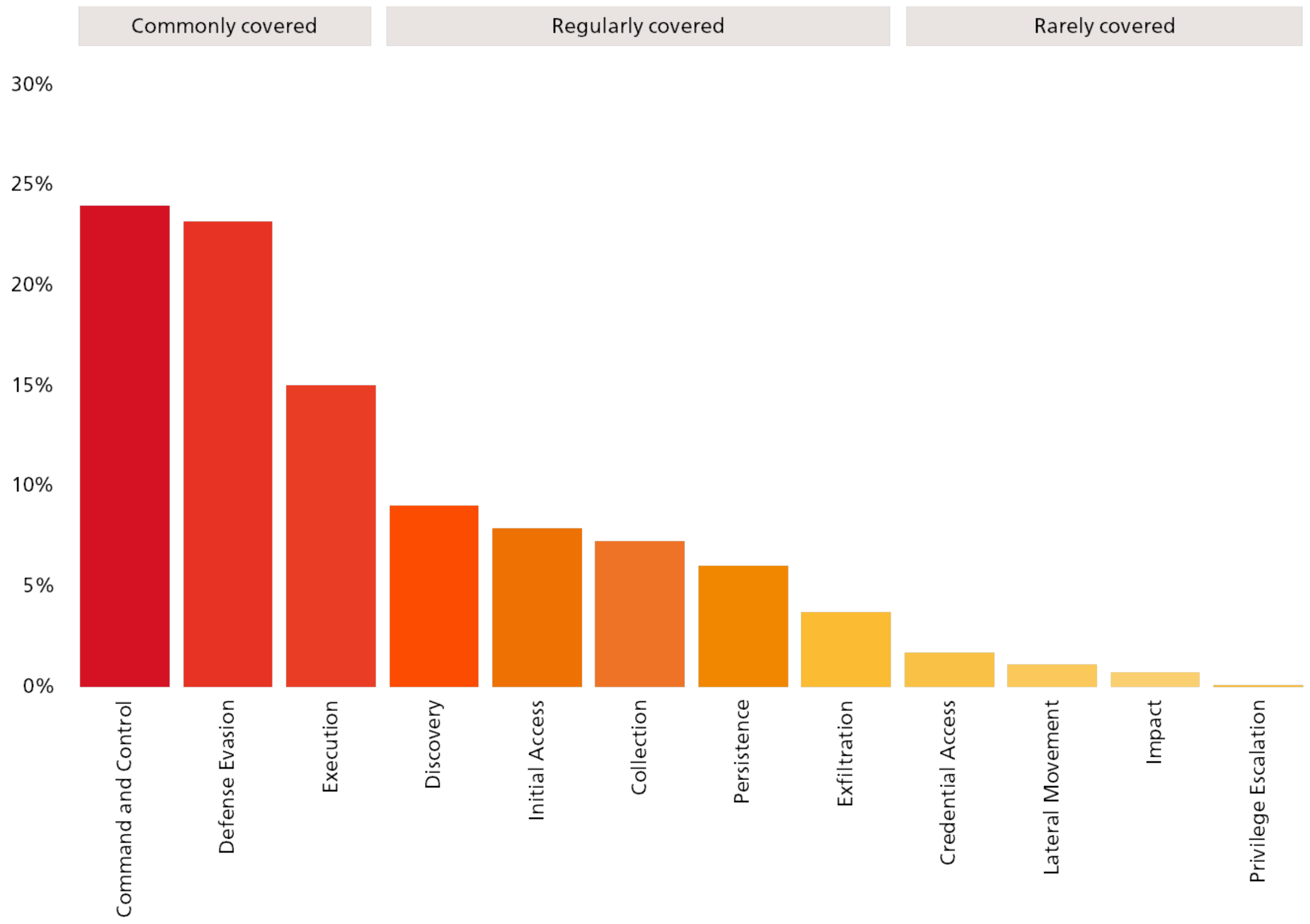
- Tactics that are **commonly covered** are Command and Control, Defense Evasion and Execution. This strongly reflects the nature of our threat reporting, where we typically report on new malware from a threat group of interest, and analyse malware behaviour and C&C methods.

- Tactics that are **regularly covered** are Discovery, Initial Access, Collection, Persistence, and Exfiltration. In some cases, we will have enough information to be able to cover these parts of the ATT&CK framework – but some parts of the 'kill chain' may be elusive (for example, the initial access technique(s) used is not always known).

- Tactics that are **rarely covered** in our threat reports are Credential Access, Lateral Movement, Impact, and Privilege Escalation. These tactics largely cover techniques that would only typically be seen in victim networks. Reports in which these techniques are discussed are likely to be based on insights from our incident response team. The Impact tactic is a relatively new addition to the ATT&CK Enterprise Matrix (added in 2019), and covers techniques where the attacker is seeking to "manipulate, interrupt, or destroy your systems and data"[1]. We have back-dated our report data to include tagging of these techniques. Techniques of this type do appear in our reports (e.g. those on ransomware, or Lazarus' use of wipers), but these are relatively rare. However, it is likely that the prevalence of this tactic will increase in future years, reflecting the increased willingness and capability of threat groups across the landscape to perform such actions.

**Figure 1**

Overall percentages of ATT&CK techniques appearing in our reports, by tactic heading.



# Evolution in TTP Observations

The graph below shows the **normalised frequency of ATT&CK tactic** prevalence in our reports across 2014 to 2019 inclusive. Normalisation by year accounts for variation (increase) in our research reporting output over the 2014-2019 timespan.

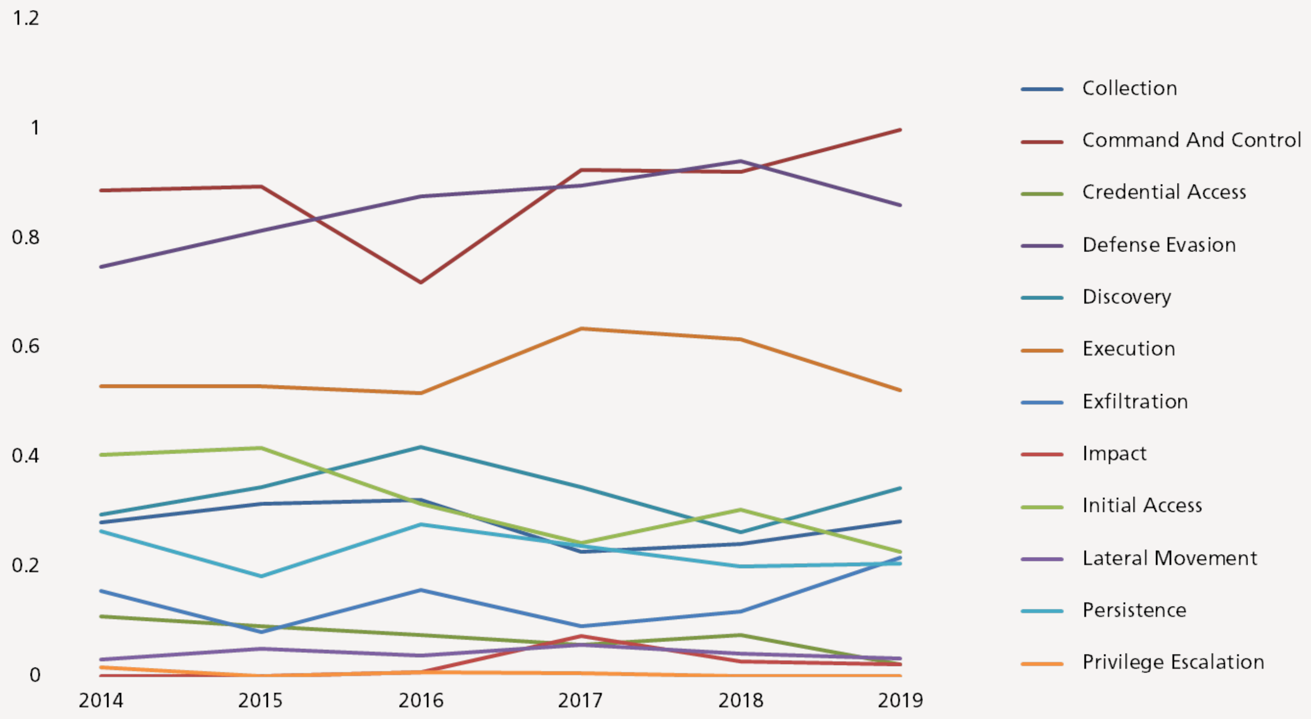


**Figure 2**

Normalised frequency of ATT&CK tactics in our research reports.

Again, it can be seen that Command and Control and Defense Evasion are the tactics which are most commonly covered in our analysis. The year-by-year data shows that these levels have been relatively consistent in our reports over time.

By analysing the data by ATT&CK technique (instead of by tactic grouping), we can gain further insight into **technique popularity in the threat landscape** and assess changes over time. The graph below shows the normalised frequency of the top five ATT&CK techniques in our data (in total), for each year 2014-2019.

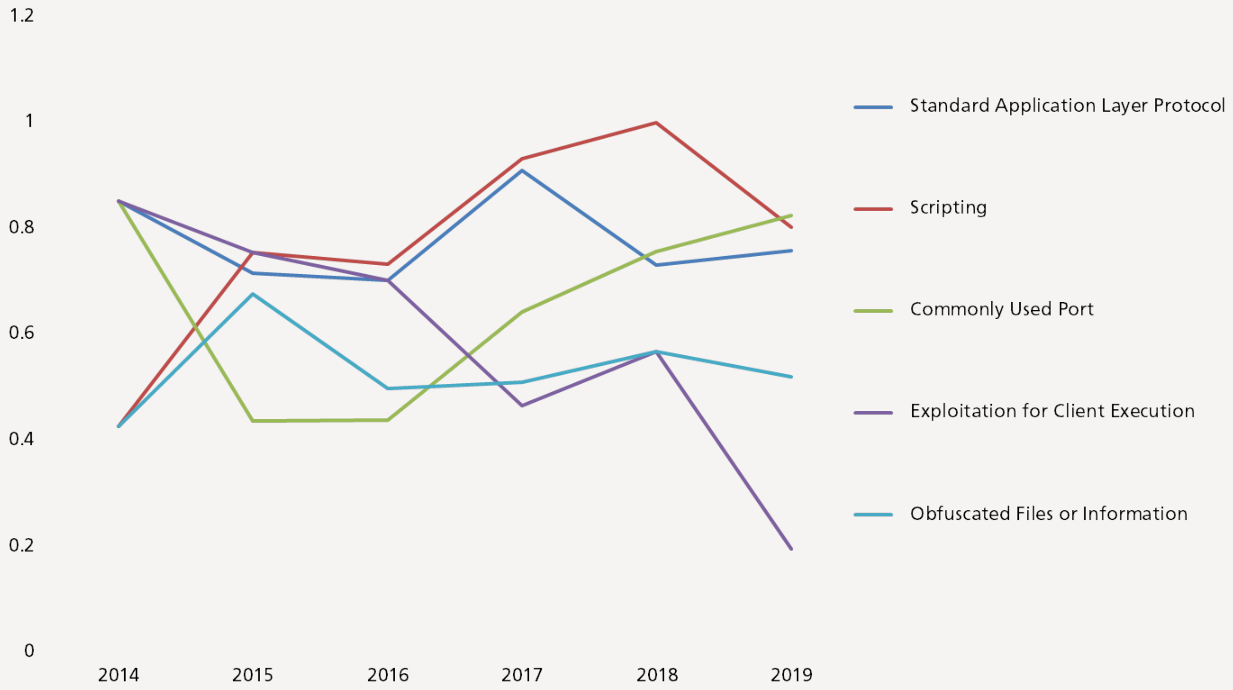


**Figure 3**
Normalised frequency of the top five ATT&CK techniques in our research reports.

**Commonly Used Port** is likely to have increased in recent years due to increased use of SSL certificates, now readily available to attackers through Let's Encrypt and other services. Most actors will have gradually shifted away from custom ports and protocols towards HTTPS – the benefits of this encryption are obvious, and it also makes incident response far trickier.

**Scripting** continues to appear frequently in our reports as attackers continue to 'live off the land', as well as using penetration testing tools to simplify their attacks and blend in. Over time, attacks have generally progressed towards multi-stage deployments as opposed to a single backdoor that is deployed immediately.

Many infection chains involve obfuscated files and information, which explains why **Obfuscated Files** or **Information** is a prevalent technique. The Lazarus group is of special note here, given the group's extensive use of packed malware.

In the graphic below, we chart the biggest increases and decreases in **ATT&CK technique frequency** that we have seen between 2014 and 2019.

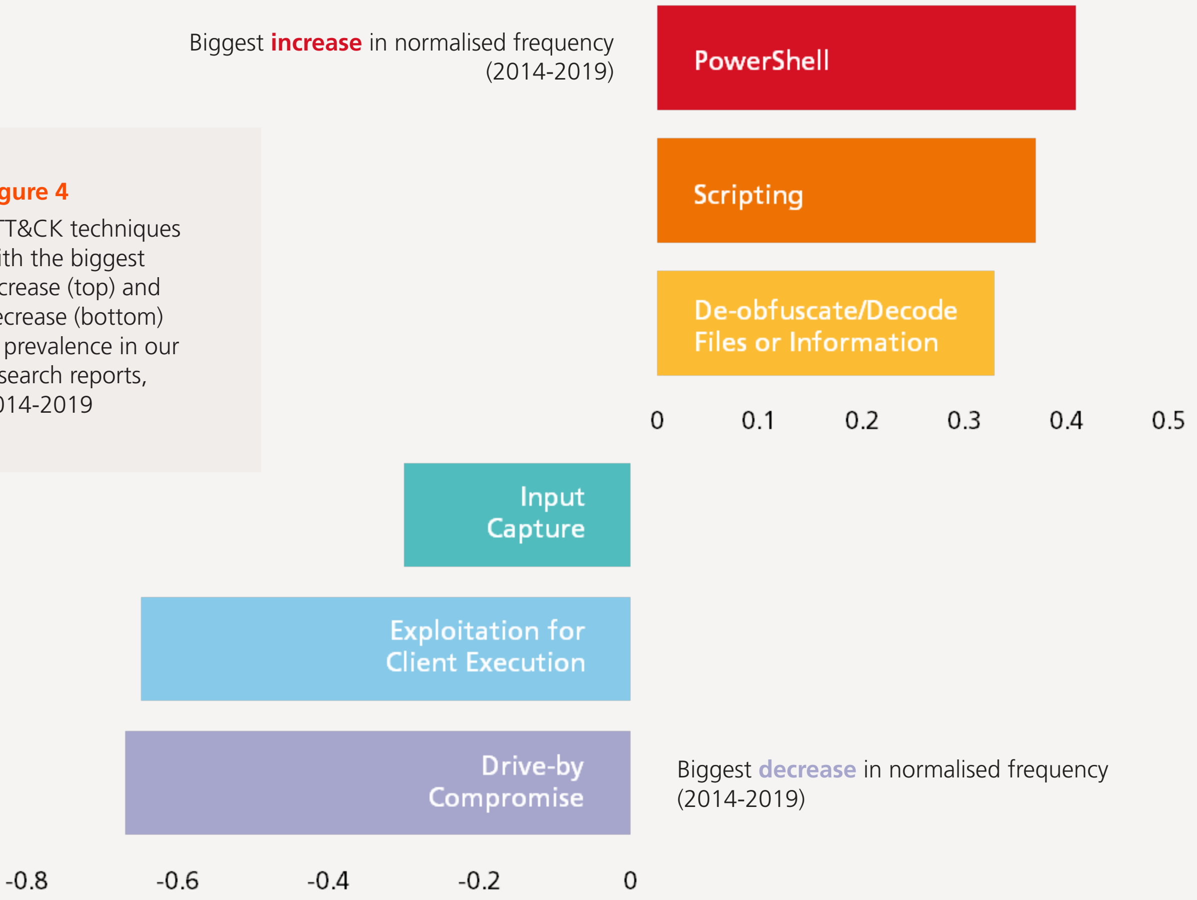


**Figure 4**
ATT&CK techniques with the biggest increase (top) and decrease (bottom) in prevalence in our research reports, 2014-2019

## The largest increases were seen in two related techniques: Scripting and PowerShell.

More groups are shifting to living-off-the-land techniques that includes the increasing use of **PowerShell.** It's interesting that in 2014, we saw no mentions of PowerShell in any of our reporting.

Drive-by compromise has decreased significantly in our data. Also known as watering-holes in more targeted cases, this attack type traditionally relied on vulnerabilities in Shockwave Flash or Java to deliver and execute malware on systems. So called exploit-kits were common a few years ago, but are now less frequently seen. Improved browser defences, fewer vulnerabilities, and shifting attacker trends have resulted in the decrease observed, although the technique is still used in some cases. Exploitation for client execution has likely decreased in line with increased use of social engineering and macros, rather than exploitation of client software (Java, Adobe Flash, etc.).

The significant increase and decrease seen in specific techniques over time is worth highlighting further.

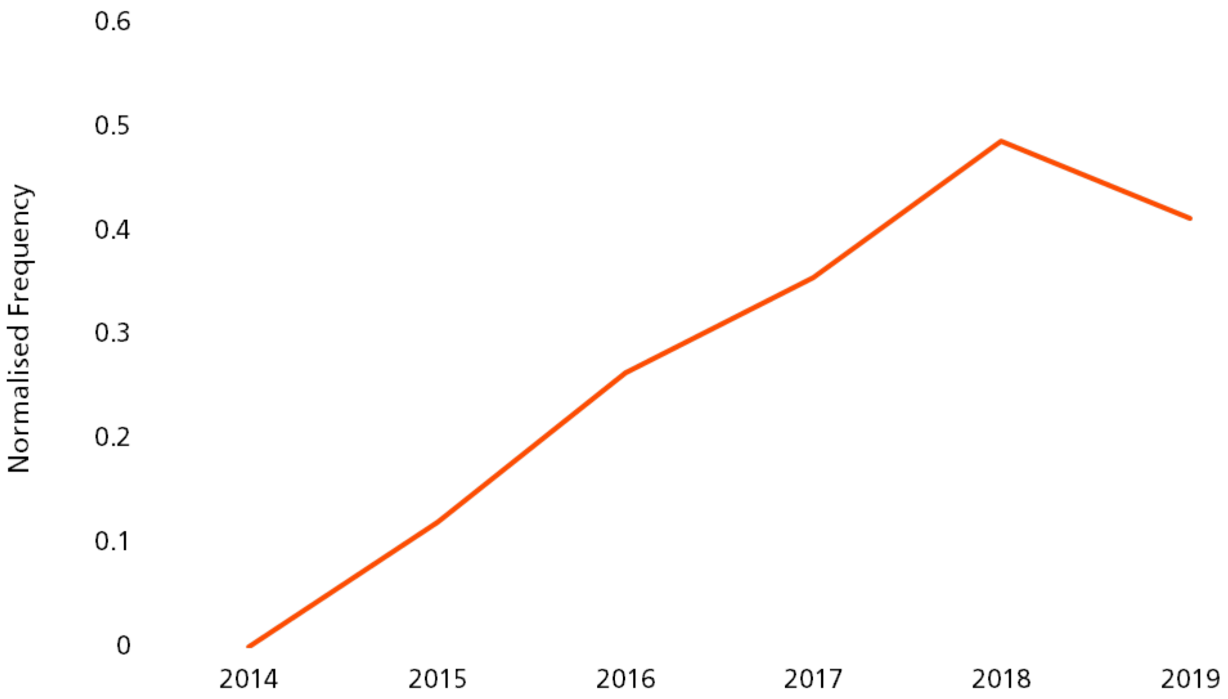


**Figure 5**

Prevalence of the PowerShell technique in our reports.

Following a rise and rise since 2014, Powershell remained a very prominent technique in our 2019 data, but may have levelled off to a degree. This may reflect a 'peak' in popularity for PowerShell – potentially due to increased awareness and detection of PowerShell and threat actor use of penetration testing tools. However, this can only be hypothesised, and additional data (including future data) would be needed to confirm this.

**Drive-by Compromise** has continued to decline in prevalence in our reporting, and in fact was absent from our 2019 data[2]. However, the technique is still being used, but is relatively rare. In 2019, Chinese threat groups used watering holes to target mobile device users from specific populations with novel exploits[3]. Moreover, in 2020, we are tracking active use of watering holes – by the Snake group, as well as MuddyWater. We expect to see a small increase in this technique next year.

In terms of **cryptographic protocols** when used in C&C, standard protocols (TLS) continue to dominate over custom cryptographic protocols. However, high-end threat groups such as Lazarus and Snake are still fond of using custom protocols in different aspects of C&C.

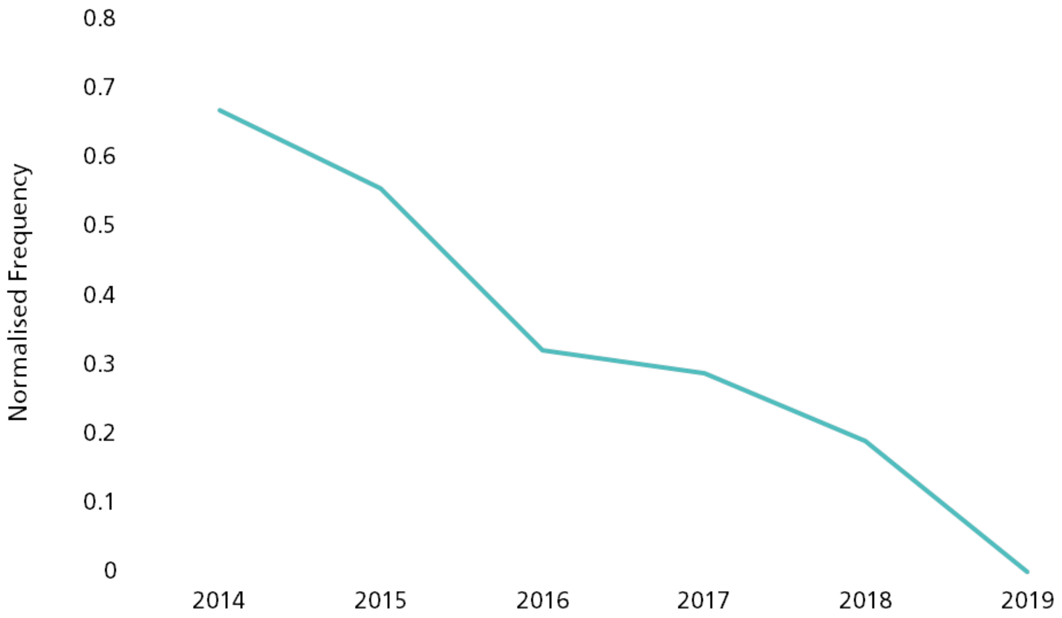


**Figure 6**
Prevalence of the Drive-by Compromise technique in our reports.

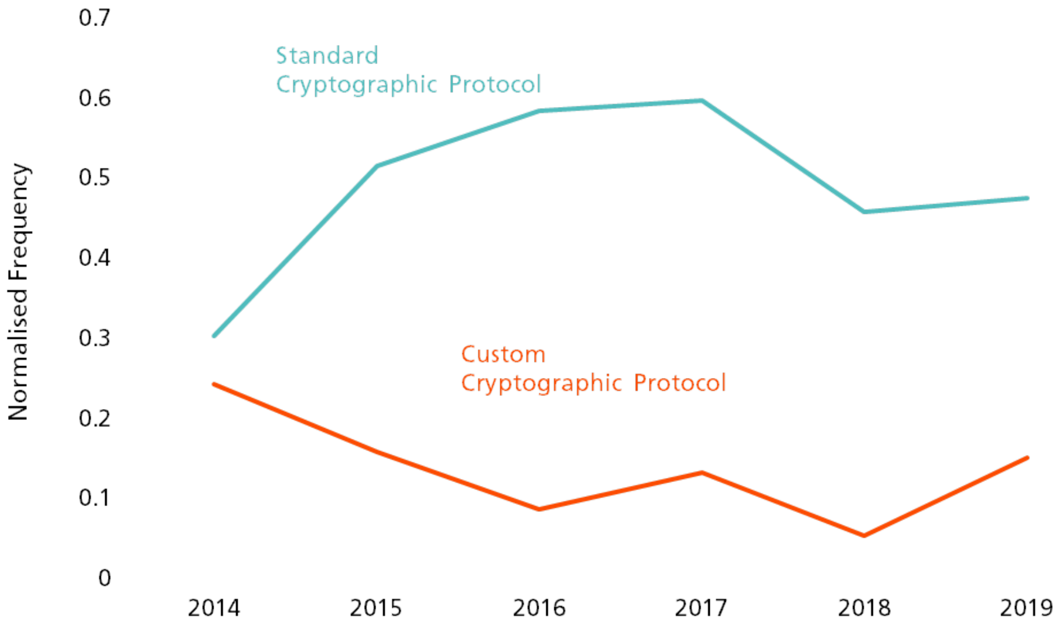


**Figure 7**
Prevalence of standard and custom cryptographic protocols for C&C in our reports

# Analysis by Threat Group Category

Another angle to analyse the data from is by looking at differences in ATT&CK TTP prevalence by **threat group category.**

Our threat intelligence research is focused on state actors from Russia, China, Iran and DPRK, as well as criminal threat actors.

In the table below, the top 20 techniques in our data overall are listed, together with their rank in prevalence in our reports covering different threat actor categories.

| | | Rank in Category | | | | |
|---|---|---|---|---|---|---|
| | **Top 20 Techniques Overall** | **Russia** | **China** | **Iran** | **DPRK** | **Criminal** |
| **1** | Standard Application Layer Protocol | 1 | 3 | 2 | 5 | 5 |
| **2** | Scripting | 3 | 8 | 1 | 2 | 1 |
| **3** | Commonly Used Port | 3 | 1 | 6 | 3 | 5 |
| **4** | Exploitation for Client Execution | 5 | 11 | | | 4 |
| **5** | Obfuscated Files or Information | 5 | 15 | 7 | 1 | 5 |
| **6** | Spearphishing Attachment | 10 | 5 | 5 | | 2 |
| **7** | System Information Discovery | 9 | 2 | 15 | 7 | 9 |
| **8** | Standard Cryptographic Protocol | 2 | 12 | 7 | 5 | 11 |
| **9** | Data from Local System | 5 | 4 | 10 | 12 | 11 |
| **10** | User Execution | 5 | | 4 | | 3 |
| **11** | Registry Run Keys/Startup Folder | 19 | 8 | 12 | | 15 |
| **12** | Drive-by Compromise | 13 | | 15 | 16 | |
| **13** | Command-Line Interface | 14 | 6 | 15 | 3 | |
| **14** | Input Capture | 17 | | 7 | | 15 |
| **15** | PowerShell | | | 3 | 8 | 11 |
| **16** | Process Injection | 11 | | | 8 | |
| **17** | Exfiltration over C&C Channel | 11 | 14 | 19 | 12 | |
| **18** | Masquerading | | 12 | | 12 | 5 |
| **19** | Uncommonly Used Port | | 15 | 12 | | 11 |
| **20** | Spearphishing Link | 20 | | | | 15 |

# Key Points

Some of the key points that emerge from this data are as follows:

- The top three techniques **(Standard Application Layer Protocol, Scripting, Commonly Used Port)** are popular among all threat categories considered here. Although these techniques reflect the overall focus of our analysis, it could also be argued that these constitute key building blocks of attacker activity in the threat landscape today. The trend toward scripting (including 'living off the land') and use of standard and common protocols/ports all make sense in terms of attackers looking to blend their activity in with legitimate host and network activity.

- Beneath the top three, variability comes in across different threat categories. For example, the fourth most common technique overall, **Exploitation for Client Execution,** does not feature in the top 20 techniques for Iranian or North Korean actors, who tend to prefer PowerShell and other living-off-the-land techniques rather than exploitation of software vulnerabilities.

- **The DPRK rankings (dominated by our Lazarus group reporting) are quite distinct:**

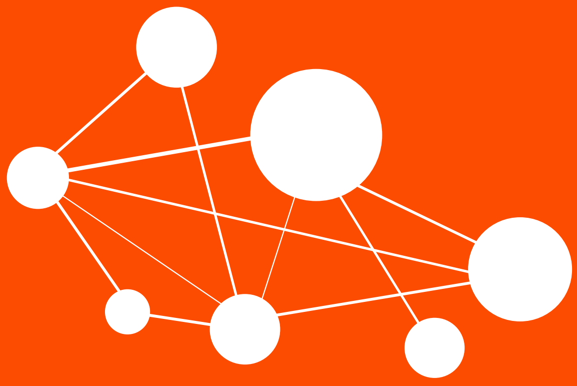
  - **Obfuscated files or information** is the most commonly described technique in activity from the DPRK nexus, in part reflecting Lazarus' preference for packed malware.
  - **Spearphishing attachment** is missing from the top 20 for DPRK groups. This reflects the fact that it is often hard to recover the full infection chain for Lazarus activity, and that initial access methods used in Lazarus campaigns remain more poorly understood than other top-tier groups.

- Iranian TTPs are generally considered of a lower sophistication than other major threat nexuses – and this is borne out to an extent in the data, where both **Scripting** and **PowerShell** are ranked highly.

- As discussed previously, **PowerShell has risen significantly in prevalence over the years,** but when broken down by category, it can be seen that it is only popular with Iranian, North Korean, and criminal operators. For Russian and Chinese groups, PowerShell is outside the top 20 most commonly reported techniques.

- **Spearphishing attachment comes up commonly in reports of criminal activity (ranked 2nd).** This is likely to be because this is easier to identify in these cases. Criminal campaigns often use malicious attachments, but they are also more readily reported/uploaded to sandboxes, etc., when compared with campaigns from state actors. Criminal activity also features a higher degree of **Masquerading,** reflecting a generally lower degree of sophistication in **Defense Evasion,** where other more sophisticated techniques are possible.

Standard Application Layer Protocol, Scripting and Commonly Used Port are popular among all threat categories.



# ATT&CK Enterprise Matrix Comments

In our analysis, a considerable number of ATT&CK techniques have never appeared in our reporting - approximately 40%. On first glance this may indicate that the ATT&CK matrix has a large number of redundant or un-used techniques, and that refinement and simplification may be in order. On the other hand, and almost certainly the case in some instances, these gaps will reflect the 'lens' through which we conduct our threat intelligence research and reporting – with a focus on malware and attacker C&C communications. MITRE's philosophy has always been to base their matrices on techniques that are observed in the wild; collation of and comparison of prevalence data from different sources in industry and government could lead to refinement in future.

The MITRE ATT&CK Matrix has recently evolved to include 'sub-techniques' to provide more granularity, addressing the fact that technique descriptions vary in breadth. Some tactics have also been added and removed, reflecting that the ATT&CK Matrix is still being evolved to best harness its usefulness for cyber defence.

Click here to visit the MITRE website and find out more

## Conclusions

The MITRE ATT&CK Matrix is a very useful resource for many purposes. We have shown above that historic analysis of techniques across our threat research over the years can emphasise trends, which then provide a degree of quantification to high-level observations about the threat landscape – highlighting techniques that have increased and decreased in popularity, as well as tangible differences in technique frequency across different threat nexuses.

As the community continues to increase its adoption of the MITRE ATT&CK Matrix, it is likely that data fed back in to MITRE will result in further evolutions to the matrix, which will improve its usefulness. The data that we have analysed here strongly reflect our approach to threat intelligence research and emphasis on malware samples as a primary source for investigations. Aggregation of techniques from teams that have different approaches and telemetry would ultimately result in a more holistic view of the threat landscape, and the ATT&CK matrix provides a great opportunity for the community to do this.

We are

**BAE SYSTEMS**

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

## Appendix

[1] https://attack.mitre.org/tactics/TA0040/

[2] While some of our 2019 reports were focussed on malware that was likely to have been delivered from watering holes, we could not confirm this from our visibility and thus did not tag them with the Drive-by Compromise technique.

[3] https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

[4] https://attack.mitre.org/beta/matrices/enterprise/

BAE Systems, Surrey Research Park,
Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/cyber

linkedin.com/company/baesystemsai
twitter.com/baesystems_ai

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

CREST
Assured Service Provider
in association with
National Cyber Security Centre

Victim of a cyber attack?
Contact our emergency response team on:

| | |
|---|---|
| UK: | 0808 168 6647 |
| International: | +44 (0) 330 158 5263 |
| Email: | cyberresponse@baesystems.com |