Title: Pcap Analysis

Group/Name: Aimé Fraser

Indicators and Technical Details

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
	A GoodCorp Executive opened a spearphishing attachment.	T1566.001 Spearfishing Attachment	
	Files are encoded	T1132.001 Data Encoding	This is a recreation of events. The analyst did not have logs or files to prove this hypothesis.
Packet 1	Source MAC 00:08:02:1c:47 DNS request returns 20:e5:2a:b6:93:f1 as threat actor's MAC.		Source IP 10.9.1.101 Destination IP 95.213.165.40
	Evolving IP addresses	T1568.002 Dynamic Resolution	IP can be unique to an attack, though the domain name may be seen in other attacks.
Packet 6	Get request to the attacker		Krtew5f[.]com is one of the indicators provided for IcedID.
Packet 8	File downloaded		File is executable: contains the string "cannot be run in DOS mode"
	Scheduled task to boot	T1053.005 Scheduled Task	Schedules to start at boot to lock in persistence,
	Browser Hijacking	T1185 Browser Session Hijacking	IcedID has used web injection attacks to redirect victims to spoofed sites designed to harvest banking and other credentials. IcedID can use a self-signed TLS certificate in connection with the spoofed site and simultaneously maintains a live connection with the legitimate site to display the correct URL and certificates in the browser.
	Brute force password guessing	T1110 Brute Force	Moves laterally by brute-force guessing the passwords of other machines,
	Exfiltration of banking data	TA0010 Exfiltration	

Executive Summary

A senior executive at GoodCorp fell prey to a spearphishing email and may have installed the known banking Trojan IcedID.

A member of the Security Operations team conducted a limited threat intelligence analysis of the available indicators before escalating it for additional threat analysis based. This more detailed analysis is outlined here. The conclusion is that IcedID was executed on the computer. IcedID is designed to cleverly steal banking, payment, and payroll credentials from financial institutions and corporations. When the user logs into certain sites flagged by the threat actor, IcedID throws up a decoy site that looks exactly like

the site familiar to the user. As the user types in credentials, the malicious software saves the credentials and passes the traffic through to the real site. Sometime later, the attacker will exfiltrate the data and use it to automate payments to their own accounts.

The affected computer should be isolated immediately and analyzed for additional malware, as the creators of IcedID are known to work with the creators of Emotet and other malware. Additionally, the network/system level mitigation and detection steps from MITRE ATT&K should be implemented to safeguard against additional attacks.

This analysis is based on the pcap, the indicators provided by the SOC team, and open-source intelligence.

Technical Summary

Most phishing emails are easy to spot. Their poor grammar, typos, and bad graphic design clearly indicate they are not what they purport to be. IcedID is different. Its finely crafted phishing emails are virtually indistinguishable as fakes, even compared to the communications put out by world-class financial institutions. The fake emails and proxy websites IcedID uses are as professional, fast, and functional as the real thing.

IcedID is also very good at hiding from computer operating systems and network security checks. It uses layers of encoding obscure the nature of its files. As a result, many antivirus and EDR solutions don't recognize it as malicious. Every installation is slightly different, so identifying IcedID by hashes or signatures doesn’t work very well. IcedID also uses Dynamic DNS to change its IPs, making it challenging to block particular IP addresses. However, traditional indicators of compromise aren't useless against it, and there are functional hallmarks we can use to identify IcedID.

Here's how researchers have shown it works. After the email is opened and the file is installed, IcedID establishes persistence by hooking several API functions via DLLs. Once in place, it creates an instance of svchost.exe and then replaces the svchost.exe code with its code. It will appear as one of many legitimate instances of svchost.exe. Since it masquerades as a normal process, most antivirus or blocking software will ignore it. Then it creates a startup task to execute the binary at every boot.

Now up and running, it waits for a browser to launch. It identifies the browser type, injects shell code into it, and modifies some of the browser's security protections. As a result, the malware "views" all browser activity, watching for financial transactions it can exploit.

It does this by setting up a local proxy server that receives all the browsing traffic and identifies opportunities for stealing banking credentials, payment card details, and other financial information. All web traffic flows through the proxy onto the web. When a user visits a banking site, the evil browser goes into action and serves up its own recreation of the login. The trojan saves the login and other potentially useful user data.

The browser presents fake banking sites so well-crafted that most users can't distinguish them from the real thing. The process is seamless to the user, as the software gathers the information and quickly passes it on to the actual site, where the transactions occur apparently normally. When the evil browser gets

what it needs, it seamlessly drops the user on the real site. Later, it exfiltrates this data to the C2 server so the bad guys can use it to automate payments to their own accounts.

Once it's gained a foothold in a single machine, IcedID spreads throughout the network using brute-force password attacks to gain access to additional hosts and banking credentials.

IcedID targets financial institutions, payroll, credit card companies, and corporations with significant payroll and accounts payable. Hence the focused attack on GoodCorp's CFO.

Findings and Analysis

The security team provided lists of indicators of compromise for this analysis. Of the domains provided as hosts for the DLL, one (krtew[5f].com 95.213.165.4) showed up in the pcap. Note the source and destination MACs and IPs. They will not change no matter the web address.

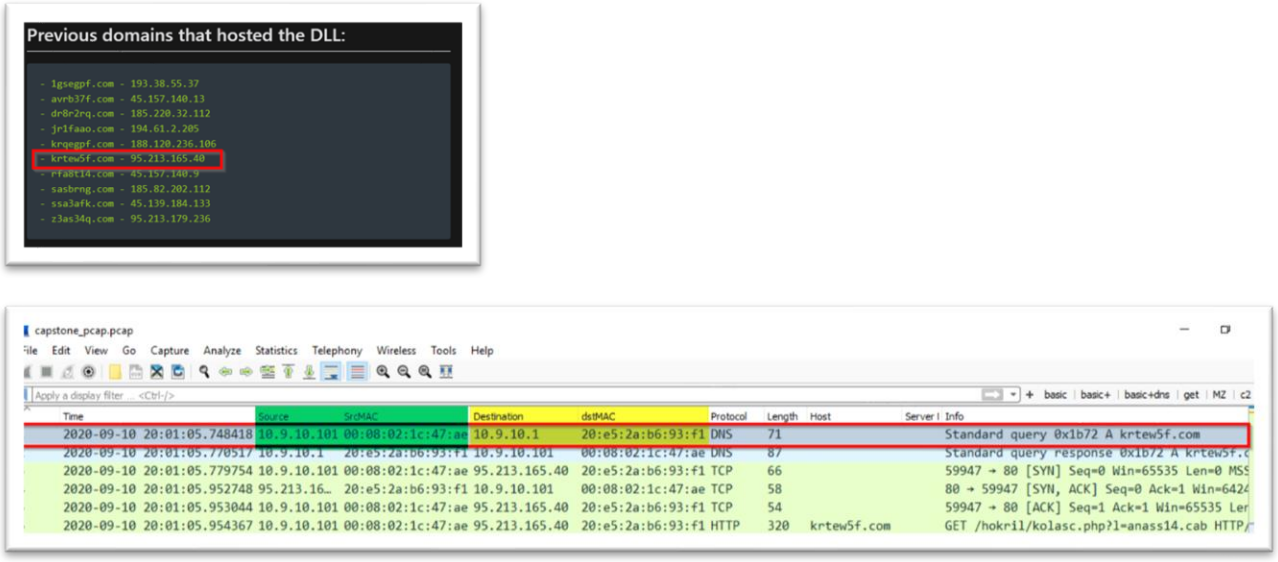
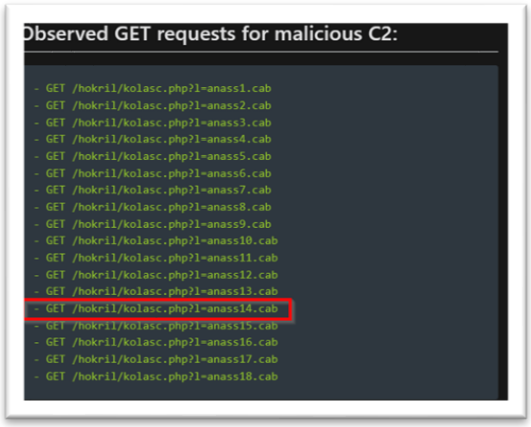


Figure 1. Top shows the indicator provided, the lower shows it in the pcap. Note the source and destination MACs and IPs.

A GET request was made to the site and downloaded a .cab file from the list -- /hokril/kolasc.php[?]l=anass14.cab. The indicator is in the pcap.



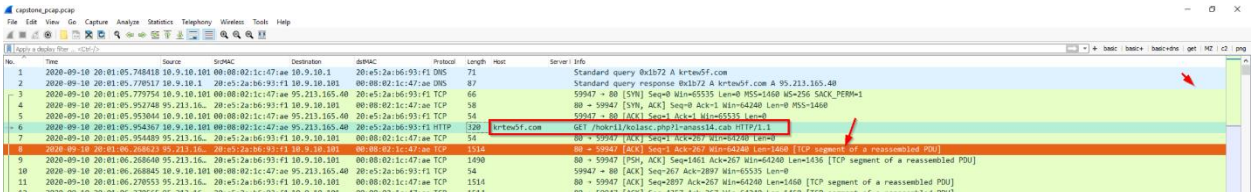
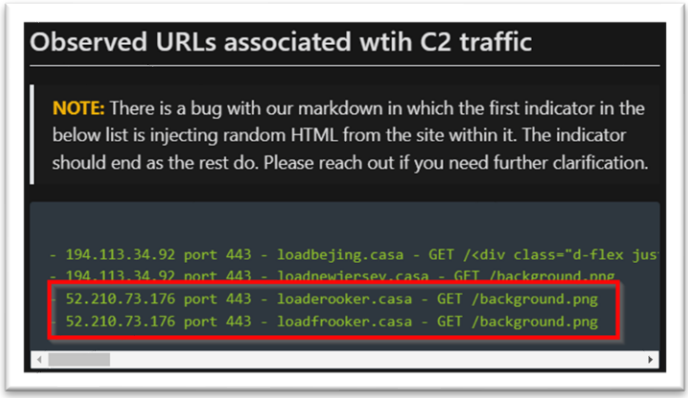


Figure 2. A GET request in the indicators is in the pcap. The orange color highlights files containing the phrase "cannot be run in DOS mode," indicating malicious code.

No URL associated with C2 traffic matched precisely, but one URL was very close. -- loadflooker[.]casa. This can be the result of dynamic DNS.



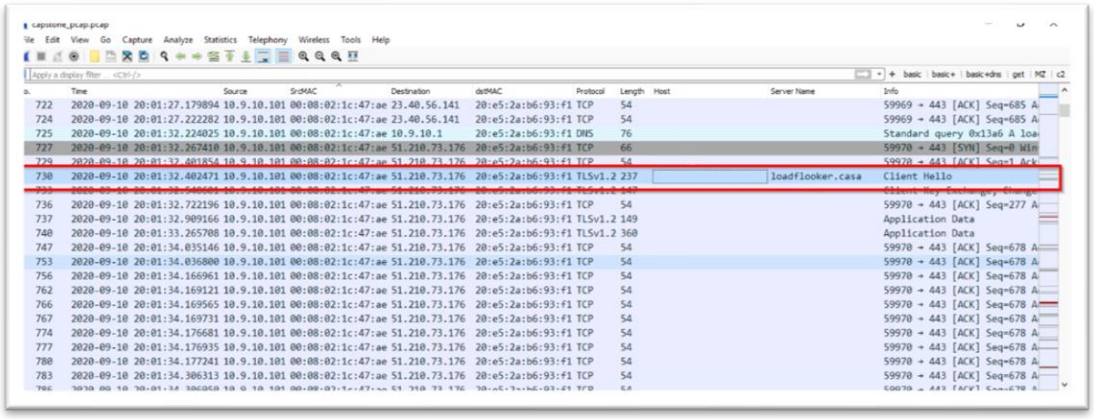
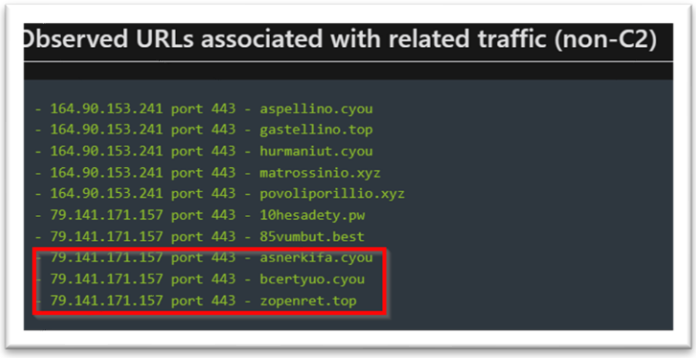


Figure 3. Another Indicator on the list appears in the pcap.

This GoodCorp infection also uses a few URLs associated with related traffic -- asnerkifa[.]cyou, bcertyuo[.]cyou, and zopenret[.]top.



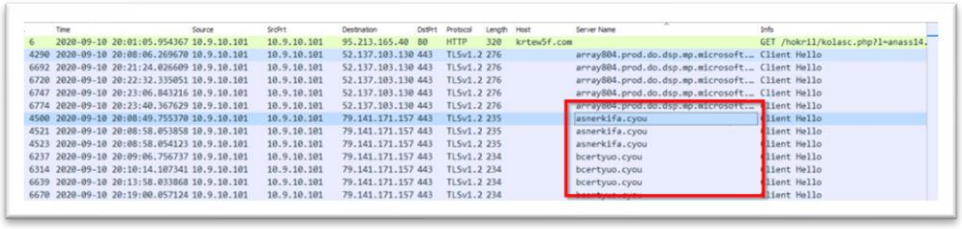
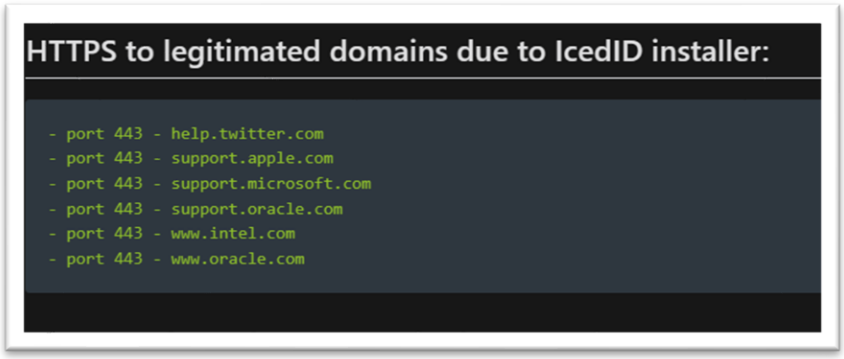


Figure 4. Sites on the list of Observed DLLs are in the pcap. Not shown is zopenret[.]top, which appears elsewhere.

The User Agent String for bcertyuo[.]cyou does not show legitimate certificate information, suggesting that it is a malicious site.

Figure 5. The User Agent String for the site does not show legitimate certificate information.

The SOC-provided list of ”legitmated [sic] domains due to IcedID installer" shows the names the legitimate names used to obfuscate the C2 server. Despite the various names, the source and destination MAC addresses are always the same -- for the GoodCorp host and the C2 server. This is true for every domain in the pcap; save the first few until the download is complete. This shows the traffic sent to the proxy server, no matter the URL.



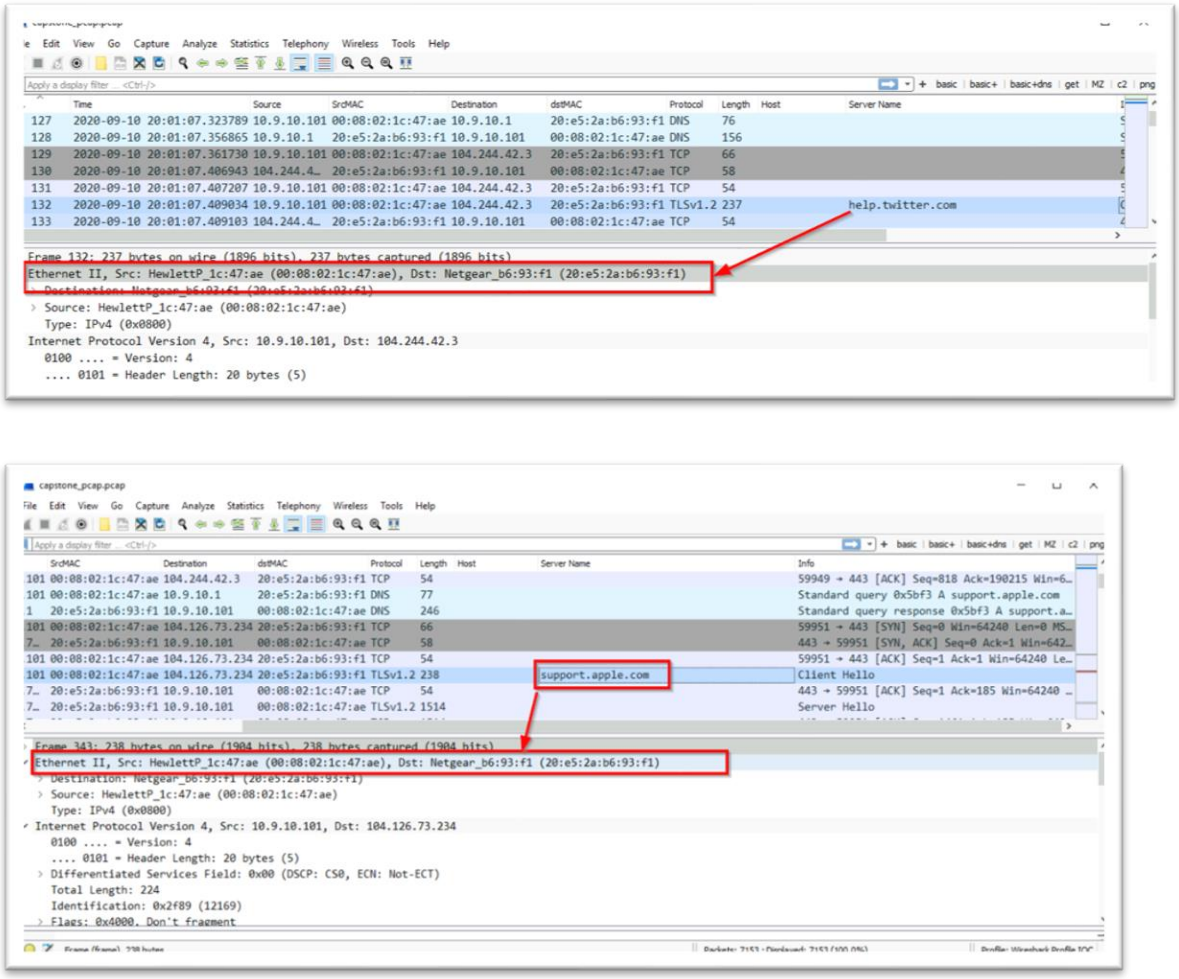


Figure 6. No matter what the domain name or IP, the domain name remains the same.

Though none of the SHA256 indicators were present, AnyRun gave the SHA 256 of the .cab file as 14A26870B13D0BB57B4847728159C4F62FA4E6D734811CAC644CB8C387C2892B. No surprise that it rated 10 out of 10 malicious.

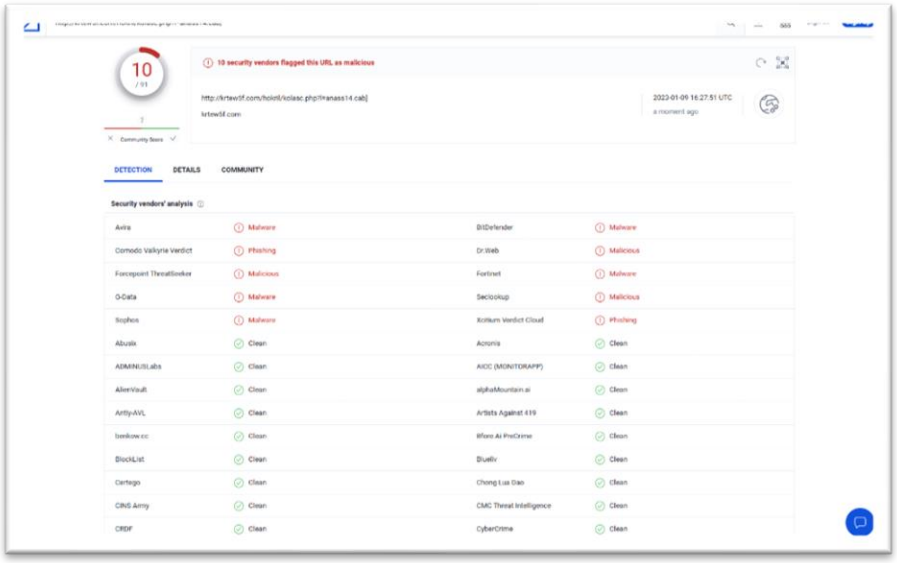


Figure 7. No surprise that Virus Total found the .cab file to be 10our of 10 malicious.

This infection is clearly IcedID and poses a significant risk to the business. GoodCorp's banking and payment process is compromised, which could have financial, operational, and reputational repercussions.

Remediation and Recommendations

Remove the infected machine from the network, reset it with a clean backup, and change the user passwords.

Create signatures and Yara rules to hunt for these indicators throughout GoodCorp's network.

In addition, consider each of the following MITRE ATT&K mitigations and detections.

M1018 User Account Management

Since browser pivoting requires a high-integrity process to launch from, restricting user permissions and addressing Privilege Escalation and Bypass User Account Control opportunities can limit the exposure to this technique.

M1052 User Account Control
Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL search order hijacking.

M1017 User Training
Close all browser sessions regularly and when they are no longer needed.

DS0028 Logon Session
Authentication logs can be used to audit logins to specific web applications but determining malicious logins versus benign logins may be difficult if activity matches typical user behavior.

DS0009 DLL Injection
Monitor for changes made to processes that may inject dynamic-link libraries (DLLs) into processes to evade process-based defenses and possibly elevate privileges.

DS0017 Command Execution
Monitor executed commands and arguments that may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.

DS0022 File Modification
Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including the startup folders.

M1049 Antivirus/Antimalware
Anti-virus can be used to automatically quarantine suspicious files.

M1040 Behavior Prevention on Endpoint
On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Visual
Basic and JavaScript scripts from executing potentially malicious downloaded content.

M1045 Code Signing
Where possible, only permit the execution of signed scripts.

M1038 Execution Prevention
Use application control where appropriate.

M1026 Privileged Account Management
When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.

M1021 Restrict Web Content
Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.

DS0017 Command Execution Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script. Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used.

DS0011 Module Load
Monitor for events associated with scripting execution, such as loading modules associated with scripting languages (ex: JScript.dll or vbscript.dll).

DS0012 Script Execution
Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible, to determine their actions and intent.

M1031 Network Intrusion
Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.

DS0029 Network Traffic
Monitor for network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.

M1036 Account Use Policies
Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial-of-service condition and render environments unusable, with all accounts used in the brute force being locked out.

M1032 Multi-factor Identification
Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.

M1018 User Account Management
Proactively reset accounts known to be part of breached credentials immediately, or after detecting brute force attempts.

DS0002 User Account
Monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. It is difficult to detect when hashes are cracked since this is generally done outside the scope of the target network.

--End--