Attack Graph Response to US CERT AA22-152A: Karakurt Data Extortion Group

By AttackIQ Adversary Research Team

Published: 2022-06-03 · Archived: 2026-04-05 14:03:22 UTC

Earlier this week we published a blog post on the release of a new AttackIQ assessment addressing the ingress of tools and malware associated with the Karakurt Data Extortion Group recently highlighted by US-CERT Alert AA22-152A. Today we are following up with the release of an in-depth attack graph that fully emulates their tactics, techniques, and procedures.

Karakurt is a financially motivated adversary focused on data extortion that have already affected more than 40 organizations across multiple industries and regions. Based on available intelligence, we have observed that the adversary is primarily focused on data theft for subsequent extortion, and not on traditional ransomware encryption or destructive attacks.

Validating your security program performance against this type of attack is paramount in reducing risk. By using this new attack graph in the AttackIQ Security Optimization Platform, security teams will be able to:

1. Evaluate security control performance against common persistence, discovery, and data exfiltration techniques.
2. Assess security posture for the techniques used by an actor focused on data theft and the extortion of victims with threats to publicly release data.
3. Continuously validate detection and prevention pipelines against actor activity that may have variable initial access methods but a common hands-on keyboard approach.

Attack Graph Emulation of Karakurt Techniques

The Karakurt threat actors are cybercriminals who typically gain access to victim networks from various initial access brokers using stolen credentials or through the exploitation of common vulnerabilities like Log4Shell or Zerologon. Our attack graph emulation starts after that initial access has already been achieved.

Once inside their target of opportunity, they focus on establishing persistence via Cobalt Strike and establishing a network connection with their command and control infrastructure.

Ingress Tool Transfer (T1105): Download and save samples of the actor's phishing documents and Cobalt Strike malware.

Application Layer Protocol (T1071) and Fallback Channels (T1008): Emulate command and control connectivity with failover options for HTTPS, HTTP, and DNS protocols.

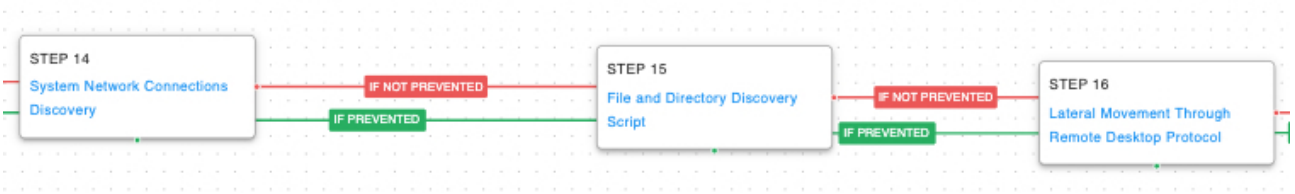
Windows Service (T1543.003), Registry Run Keys (T1547.001), and Windows Management Instrumentation (T1047): Cobalt Strike has a plethora of persistence options; our attack graph will try a subset of these methods to find a successful foothold.

Now that persistence has been established, Karakurt focuses on gathering additional credentials that can be leveraged to move laterally to other systems or access remote external servers.

Account Discovery (T1087): Use living off the land commands like "net user" to obtain a list of additional accounts known to the infected host.

OS Credential Dumping (T1003): Karakurt has been observed using Mimikatz to dump passwords and hashes for Windows accounts.

Armed with their new credentials the actor is going to start the discovery phase of their attack to find connectable hosts, files and folders of interest, which will guide their lateral movement using native operating system functionality like Remote Desktop.

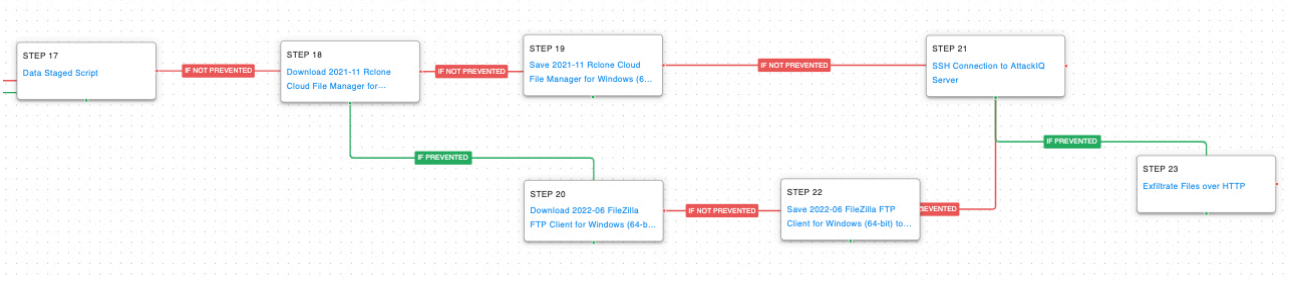


System Network Connections Discovery (T1049): Continue to leverage living off the land commands like "netstat" and "net use" to find other systems remotely connected to the initial foothold host.

File and Directory Discovery (T1083): Karakurt will be looking at the local host and remote shares to find sensitive files that can be stolen and held as ransom. Generating file and directory lists to identify data files to speed up their assessment.

Remote Desktop Protocol (T1021.001): Combining the dumped credentials and the discovered remote hosts, the actor will attempt to move laterally to another host and repeat their discovery process until they have collected enough data to exfiltrate.

Once their discovery and lateral movement actions are completed, it's time for Karakurt to begin staging the stolen data and exfiltrate it to actor owned external resources. They will attempt to use cloud providers or SFTP for bulk exfiltration. If all else fails, they can fall back to Cobalt Strike for data exfiltration over HTTP.



Local Data Staging (T1074.001): This actor prefers to conduct bulk exfiltration operations, so collecting and staging data in a single place assists with this method.

Exfiltration to Cloud Storage (T1567.002): Karakurt has been observed downloading and using command-line tool, Rclone, to exfiltrate files to 'Mega.io' or other cloud providers.

Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002): Additionally, the actor has been observed bringing FileZilla into the environment to exfiltrate data over SFTP.

Exfiltration Over C2 Channel (T1041) and Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003): If the bulk exfiltration attempts are thwarted, the actors have the option of using their Cobalt Strike backdoor to exfiltrate over an HTTP connection.

Opportunities for Extending the Attack Graph

In addition to what's already covered in the attack graph, there are two additional techniques employed by this threat actor that are also part of the AttackIQ platform. Security teams can easily extend this Attack Graph with a simple clone operation followed by the addition of these scenarios, or they can create new assessments if their environments meet the scenario requirements:

1. **Dump Active Directory Databases (T1003.003):** One high value objective for cyber threat actors is to obtain a copy of the Active Directory database so that it may be attacked offline. Karakurt has been observed dumping the NTDS.dit database from a domain controller once administrative access has been achieved. This scenario must be executed on a domain controller asset.
2. **Exfiltrate Files over SFTP (T1048.002):** Attackers, including Karakurt, commonly use covert data exfiltration methods to avoid detection. Adding this SFTP exfiltration scenario is recommended to assist in detection and prevention of this technique. This scenario requires an accessible server that supports Secure Shell and the valid credentials to access the remote resource.

Detection and Mitigation Opportunities

With so many different techniques being utilized by threat actors, it can be difficult to know which to prioritize for prevention and detection opportunities. AttackIQ recommends first focusing on the following techniques emulated in our scenarios before moving on to the remaining techniques.

1. Ingress Tool Transfer (T1105)

Stopping or identifying when the threat actor is bringing down their toolset after the initial compromise will help prevent follow-up actions those tools facilitate. Once a malicious actor has compromised an endpoint, they may attempt to transfer tools or malware onto the device using applications like PowerShell, certutil, Bitsadmin, and Curl.

1a. Detection Process

The following Sigma rules can help identify when suspicious file downloads are being conducted:

PowerShell Example:

```
Process Name == (Cmd.exe OR Powershell.exe)
Command Line CONTAINS ((“IWR” OR “Invoke-WebRequest") AND “DownloadData” AND “Hidden”)
```

certutil Example:

```
Process Name == Certutil.exe
Command Line Contains (“-urlcache” AND “-f” AND “http”)
```

Bitsadmin Example:

```
Process Name == Bitsadmin.exe
Command Line CONTAINS (“/transfer” AND “http”)
```

Curl Example:

```
Process Name == Curl.exe
Command Line CONTAINS (“http” AND “-o”)
```

1b. Mitigation Policies

MITRE recommends the following mitigations:

- M1031

2. Windows Service (T1543.003), Registry Run Keys (T1547.001), and Windows Management Instrumentation (T1047):

Persistence is a key inflection point in an actor's attack lifecycle. Concerned about their potential loss of access, they are going to take steps to ensure they will remain on the infected host after reboots or partial remediation efforts. Disrupting their ability to maintain their foothold will help prevent their immediate return.

2a. Detection Process

The following rules can help identify when those persistence mechanisms are being set.

```
Service Creation:
Process Name == (Cmd.exe OR Powershell.exe)
Command Line CONTAINS ('sc' AND 'create' AND 'start= "auto"')
```

```
Registry Run Keys:
Process Name == powershell.exe
Command Line CONTAINS ("Set-ItemProperty" AND ("HKLM" OR "HKCU") AND "Software\Microsoft\Windows\Cur
Process Name == ("cmd.exe" OR "powershell.exe")
Command Line CONTAINS "reg.exe" AND "add" AND ("HKLM" OR "HKCU") AND "Software\Microsoft\Windows\Cur
```

Windows Management Instrumentation:

```
Source == "WinEventLog:Microsoft-Windows-WMI-Activity/Operational"
EventCode == ("5859" OR ("5861" AND ("ActiveScriptEventConsumer" OR "CommandLineEventConsumer" OR "C
Provider != "SCM Event Provider"
Query != "select * from MSFT_SCMEventLogEvent"
User != "S-1-5-32-544"
PossibleCause != "Permanent"
```

2b. Mitigation Policies

Ensure that Group Policy enforces only authorized users or administrators are able to use tools such as cmd.exe , powershell.exe, sc.exe and reg.exe. Limiting these administrative tools to only authorized personnel will greatly limit the chance of these attacks being carried out on lower privileged users.

MITRE recommends the following mitigations for T1543.003:

- M1047
- M1040
- M1045
- M1028
- M1018

3. **OS Credential Dumping (T1003)**

Actors like Karakurt will almost always require additional usernames and passwords beyond those they started with in order to move laterally to other hosts and to find additional sensitive data. Mimikatz is an open-source tool

with regular version updates that evade many antivirus solutions. Focusing on the command line arguments and subsequent behavior is a solid foundation to limit the actor's ability to spread.

3a. Detection Process

```
Process Name == powershell.exe
Command Line CONTAINS ((“DownloadString” OR “DownloadFile”) AND “http” AND “.ps1” AND (“IEX” OR “Inv
```

3b. Mitigation Policies

MITRE recommends the following mitigations for **T1003**:

- - M1015
  - M1040
  - M1043
  - M1041
  - M1028
  - M1027
  - M1026
  - M1025
  - M1017

4. Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003)

The last possible prevention opportunity for this intrusion is when they attempt to exfiltrate collected victim data. Preventing an actor from establishing those connections to untrusted sites or identifying when legitimate services are being abused is crucial to stopping a data breach. A determined actor like Karakurt is not going to give up when one avenue fails; they will be persistent and leverage their exfil fallback options. Therefore it is key to be aggressive in responding when these alerts are triggered.

4a. Detection Process

Detecting exfiltration is well suited for IDS/IPS and DLP solutions. These products should be configured to identify sensitive files. If sensitive files, or a large amount of web traffic is sent to a rare external IP, it should be detected or prevented depending on security policies for the security control. Historical NetFlow data logging can also bubble up hosts that are experience uncommon peaks in outgoing traffic.

4b. Mitigation Policies

MITRE recommends the following mitigations for **T1048.003**:

- - M1057
  - M1037
  - M1031
  - M1030

Conclusion

In summary, this attack graph will evaluate security and incident response processes and support the improvement of your security control posture against an actor with focused operations to find and exfiltrate sensitive data. With data generated from continuous testing and use of this attack graph, you can focus your teams on achieving key security outcomes, adjust your security controls, and work to elevate your total security program effectiveness against a known and dangerous threat.

AttackIQ stands at the ready to help security teams implement this attack graph and other aspects of the AttackIQ Security Optimization Platform, including through our co-managed security service, AttackIQ Vanguard.
