The Shadows of Ghosts: Inside the Response of a Unique Carbanak Intrusion

Blog Post created by Jack Riley RSA on Dec 4, 2017

RSA Incident Response White Paper: Inside the Response of a Unique CARBANAK Intrusion

RSA Incident Response and Discovery Practice (RSA IR) analysts spend a significant amount of time engaged in the research, hunting, and effective response of advanced and persistent actors. A customer engagement early-to-mid-2017 is an excellent example of a unique case in which RSA IR successfully responded to an intrusion perpetrated by the threat actor group CARBANAK, also known as FIN7. The CARBANAK actions illustrated in this post and associated paper were observed with other RSA clients as recently as November 2017, with the methods and intelligence supplied by these publications having been used successfully to detect and track attacker activities.

Several intrusions associated with the **CARBANAK** actors have been reported within the last year, describing compromises of organizations within banking, financial, hospitality, and restaurant verticals. However, they all describe a relatively equivalent progression, with only slight deviation in specific attacker actions. The intelligence surrounding recent **CARBANAK** incidents indicate that phishing attacks have been the group's primary method of initial compromise. After gaining access to a user system, the attackers move laterally throughout the environment, conduct internal reconnaissance, establish staging points and internal network paths, harvest credentials, and move towards their intended target. However, this intrusion began with a significantly higher level of privilege

due to the exploitation of the Apache Struts vulnerability CVE-2017-5638 allowing the attackers to quickly gain administrative access within the client's Linux environment. This intrusion presented substantial challenges due to:

- The initial intrusion vector
- Unique attacker toolset
- The attacker dwell time
- The large, heterogeneous environment
- The speed with which the attackers gained administrative access
- The forensic mindfulness of the **CARBANAK** attackers

The attackers' toolset was a mix of custom tools, freely available code, and open source software utilities. RSA IR researched all 32 of the malicious files in the **CARBANAK** toolset using various publicly available and open-source resources. Six of the tools used in this intrusion were found to have been uploaded to a publicly available anti-virus aggregation site. Of these six, five have little-to-no detection or indication of malice from antivirus vendors. This observation explains why the client's signature-based host protection mechanisms were unable to identify or prevent the use of these tools.

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf599bd126a7b59d5d1f97ba89a3e71425731 peexe software-collection upx via-tor	1 / 59	2009-04-25 23:42:23	2017-09-27 07:02:16	3050	1938	392.0 KB
9d42c2b6a10866842cbb6ab455ee2c3108e79fecbffb72eaf13f05215a826765370d420948672e04ba8eac10bfe6fc9c 64bits peexe assembly	20 / 60	2017-05-20 00:53:52	2017-05-22 21:55:11	6	1	4.2 MB
e0e2c7d0f740fe2a4e8658ce54dfb6eb3c47c37fe90a44a839e560c685f1f1fae3c061fa0450056e30285fd44a74cd2a peexe	0 / 65	2016-10-04 17:09:48	2017-09-18 01:18:55	54	36	637.5 KB
3ed6749bba634ad0f5e888daf0323c85fe73f9cb8fc70c05fb42d53eb7a8b523b57dc2bc16dfdb3de55923aef9a98401 64bits elf	1 / 55	2017-05-04 17:37:30	2017-05-04 17:37:30	1	1	21.1 KB
91bde887f6956546c9a5e328e2bf90b1ca2fd28bc9fa39b84701891ee8230e81ab8bed25f9ff64a4b07be5d3bc34f26b peexe	0 / 62	2017-06-01 07:07:27	2017-06-01 07:07:27	1	1	482.5 KB
b20ba6df30bbb27ae74b2567a81aef66e787591a5ef810bfc9ecd45cb6d3d51eb3135736bcfdab27f891dbe4009a8c80 peexe signed overlay	0 / 64	2016-03-05 11:16:34	2017-07-31 10:33:23	159	122	350.9 KB

Figure 1: Findings from Public and Open Source Research of Toolset Reference

While the attackers used more than 30 unique samples of malware and tools, they also demonstrated a normalization across Windows and Linux with respect to their toolset. The toolsets they deployed can be broken down into five basic functionalities:

- Ingress/Egress/Remote Access

- Lateral Movement
- Log Cleanup
- Credential Harvesting
- Internal Reconnaissance

The ingress, lateral movement, and internal reconnaissance mechanisms used by the attackers during this investigation were not that sophisticated in and of themselves. However, when viewed in aggregate, and from an operational view, RSA observed the actors normalized their choice in toolset across the Linux and Windows environments. The attackers in this engagement primarily used modified versions of legitimate administrative tools, commonly used penetration testing utilities, and common network file acquisition tools. Though specialty malware was observed during this intrusion, the attackers used basic XOR encoding just above Layer 4 to facilitate communication, communicated via SSH tunnel directly over TCP/443, or just transmitted and received data in clear text across the network. Of the observed actions during this intrusion, none of the attacker tools, techniques, or procedures were particularly advanced. However, they were still able to bypass a significant security stack, obtain initial access and lateral access effectively, deploy malware and toolsets with impunity, and traverse over 150 systems in the span of six weeks. While, at first glance, this attack was not sophisticated in its toolset, it was sophisticated in its operationalization and agility of attackers' actions. The correlations between the Linux environment tools and the Windows environment tools are shown below:

Cross-Platform Toolsets and Purpose		
Linux	**Windows**	**Function**
Winexe	Tinyp (PSEXEC Variant)	Lateral Movement
Auditunnel (Linux Version)	Auditunnel (Windows Version)	Ingress Tunneling
PScan (Linux Version)	PScan (Windows Version)	Internal Recon
WGet (Linux Version)	WGet (Windows Version)	Toolset Download
SCP	PSCP	File Transfer

RSA IR released a white paper containing an in-depth review of this engagement, including observed attacker operational patterns, TTPs, and the techniques used during this engagement to successfully track and respond to the threat. The observations illustrated in this paper identify that not only do **CARBANAK** actors have the capability to successfully compromise various operating system environments, they have standardized and operationalized this capability. This attribute indicates strategic operational thought and effort being invested in this group's compromises, suggesting that the **CARBANAK** actors are working towards becoming a more organized, structured, resourceful, and mature threat group.

During an intrusion, **time** is the single most critical resource to an organization's security team and is the most significant indicator of determining if the security team will be successful in containing, eradicating, and remediating the extant threat. There are two specific sets of time related to an intrusion that may determine the difference between success and failure: the time that the attackers are in the environment prior to detection (dwell time), and the time it takes security teams to identify, investigate, understand, and contain the attacker's actions (response time). In this specific incident, the attacker's dwell time at intrusion declaration was 35 days, which is a significant amount of time given the level of access immediately available upon compromise. However, by utilizing the methodology and visibility described in this paper, RSA IR was able to complete containment, eradication, and remediation in *only nine days*. We also discuss

the methodology used by RSA IR to successfully detect, investigate, understand, and contain the attackers before the actors could achieve their intended goal.

The **CARBANAK** actors not only showed the capability to successfully compromise both Linux and Windows systems, they chose a toolset that was either directly cross-platform or extremely similar in both function and command line usage. This indicates a level of tactical organization and operationalization not previously observed by this actor group. Additionally, they were significantly cognizant and aware of actions taken by the security team, switching to new methods of ingress after initial compromise, detected remediation actions, and environmental migration. They were methodical in their choice of staging systems, basing the system utilized on:

- a critical function of lateral access
- or responder detection and investigation

They chose key systems based on their needs rather than systems the organization would consider 'key' assets. They ensured the toolsets they would interact with most often contained very similar functions and commands across environments in order to limit mistakes made at the keyboard. They included a method, whether manually or automatically, to remove any record of their activities. They operated with purpose, patience, planning, and most significantly, persistence.

This intrusion was successfully discovered, investigated, contained, eradicated, and remediated only due to the following reasons:

1. The organization invested in the *necessary visibility* at a host and network level to allow analysts to rapidly and effectively hunt for and investigate these types of threats.
2. The organization had invested and *empowered their personnel* to creatively and proactively hunt for, understand, investigate, and learn from threats within their environment.
3. The organization had maintained a relationship with a proven and trusted advisory practice and had worked to recreate and implement a solid and proven Threat Hunting and Incident Response methodology within their own organization.
4. The organization had a solid top-down understanding of what role Threat Hunting and Incident Response held during daily operations and security incidents, and provided the necessary support and enablement to subordinate units and analysts.

While a first look at the tools used in this engagement may appear simplistic, upon review of the entire intrusion, it becomes quickly apparent that each of them was purpose-chosen with an overall operationalized capability in mind. **CARBANAK** has shown themselves to be a coordinated and extremely persistent group of actors that are consistently moving towards more agile methods of intrusion and standardization of processes across

heterogeneous environments. They have proven their capability to use that persistence and agility to defeat or bypass organizational security controls. Even with the least advanced of their capabilities, they can be a difficult adversary to track within an environment due to their speed, efficiency, adaptability, and care in leaving little trace of any activity. However, this difficulty compounds exponentially for organizations without the necessary visibility, practices, methodologies, or trusted partner relationships necessary to effectively detect and respond to these types of threats. This white paper shows that with the necessary visibility, planning, methodology, and analyst enablement, organizations can be successful against these types of threats.

Learn more about the Carbanak/Fin7 syndicate based on unique Carbanak intrusions, and the mindset and methods used to combat them in these recent RSA Research publications.

Visibility: RSA NetWitness Suite • 86 Views

Last modified on Dec 4, 2017 6:34 PM

Tags: incident_investigations | rsa_ir | rsa incident response | security operations and breach managem... | incident discovery | methodology | intrusion | analyst report | threat intel | threat hunting | netwitness for endpoint | netwitness logs & packets | netwitness packet | incident response essentials | carbanak | fin7

Categories: RSA NetWitness Endpoint | RSA NetWitness Logs | RSA NetWitness Packets

0 Comments

Related Content

- ESA – Intrusion Detection with Windows Event Logs
- Detecting APT Using Anomalous Windows Remote Management Methods and Dynamic RPC Endpoint Mapping
- Recent resurgence in Shamoon
- ANOTHER HOLIDAY LOST … WannaCry and Wanna Decryptor
- Another great threat Profile... Shell_Crew

Recommended Content

- Investigate: Analyze Events in the Event Analysis View
- Beat the Clock & Save $$ on Your Upgrade to RSA Archer 6.x: Maximize Your Benefits with One of Two RSA Professional Services Discounts, Offer Extended Through Feb. 4, 2018
- System Security and User Management Guide for Version 10.6.5
- RSA Security Analytics System Configuration Guide
- 000033416 - Opening RSA Archer Records takes a long time to load

---