

# Here's how to guard your enterprise against ShinyHunters

 [intel471.com/blog/shinyhunters-data-breach-mitre-attack](https://intel471.com/blog/shinyhunters-data-breach-mitre-attack)

---

There is a group in the cybercriminal underground that is trying to collect troves of enterprise data the same way that millions of gamers collect Pokémon.

Since surfacing in April 2020, the group — which refers to itself as ShinyHunters — has been behind some of the most notable data breaches that have been made public. Those include breaches of [Microsoft's GitHub account](#), [photo editing app Pixlr](#), and [men's clothing retailer Bonobos](#). Intel 471 has also observed them claiming responsibility for several other breaches, including incidents impacting a sports media company, a mobile travel platform, and a website that allows musical artists to find and book gigs. As research was being conducted for this blog, the group claimed to be in possession of 70 million records with personally identifiable information that it took from telecom giant AT&T.

With figures estimating the average data breach this year is approximately \$4.4 million, we can estimate that ShinyHunters has cost companies tens of millions of dollars in damages this year.

Primarily operating on Raid Forums, the collective's moniker and motivation can partly be derived from their avatar on social media and other forums: [a shiny Umbreon Pokémon](#). As Pokémon players hunt and collect “shiny” characters in the game, ShinyHunters collects and resells user data.

While the group's targets are spread across different economic sectors, the methods by which they are obtaining organizational data follow a consistent pattern. ShinyHunters tries to obtain legitimate credentials, most likely for a company's cloud services. From there, the group will seek to target database infrastructure to gather [PII](#) to be resold on marketplaces for profit. Intel 471 has also observed ShinyHunters targeting DevOps personnel or GitHub repository companies in order to steal valid OAuth credentials. These OAuth keys are used to access cloud infrastructure and bypass any two-factor authentication processes that are in place.

Below is a further breakdown of the courses of action (CoAs) the actor could take based on TTPs identified, including the most likely courses of action (MLCoA) and the most dangerous courses of action (MDCoA) that organizations could anticipate. More MITRE ATT&CK

mapping can be found at the end of this blog.

## ShinyHunters Scenario **Most Likely** Courses of Action

## ShinyHunters Scenario **Most Dangerous** Courses of Action

### RECONNAISSANCE [TA0043]

🔥 Identify organizations using Microsoft Office 365 and search for valid accounts.

🔥 Identify third-party companies that store GitHub open authorization (OAuth) tokens.

🔥 Identify and research development and operations (devops) personnel.

### WEAPONIZATION

🔥 Identify credentials for valid accounts from leaked and/or previously stolen credential data sets.

🔥 Purchase credentials on marketplaces such as Genesis.

🔥 Use accounts to log in to cloud services.

🔥 Hack third-party companies to steal OAuth tokens, leverage them to bypass two-factor authentication (2FA) and gain access to cloud services.

🔥 Directly target devops personnel to phish valid GitHub repository credentials.

### DELIVERY [TA0001]

🔥 Directly target database vulnerabilities to access sensitive information.

🔥 Target software repositories to access application programming interface (API) keys, OAuth keys, hard-coded credentials and more.

### EXPLOITATION

🔥 Steal sensitive data such as credentials and PII.

🔥 Exploit remote service tools.

🔥 Audit source code to find vulnerabilities that can be leveraged in larger scale attacks.

### COMMAND AND CONTROL [TA0011]

🔥 Exfiltrate data via web services.

🔥 Alternate domain name system (DNS) records to redirect legitimate traffic.

🔥 Use exploited nodes as a vector and/or exit node for future attacks.

🔥 Leverage legitimate credentials and tools such as GitHub utilizing OAuth which makes it more difficult to detect.


### ACTIONS ON OBJECTIVES [TA0040]

🔥 Sell stolen data on forums for profit.

🔥 Extort, blackmail and expose information in the underground.

### OUTCOME

<ul style="list-style-type: none"> <li>🔥 <b>Confidentiality:</b> Information theft and espionage.</li> <li>🔥 <b>Integrity:</b> Modification or deletion of data from an unauthorized party.</li> <li>🔥 <b>Availability:</b> Unable to update or access the environment until it is secured and accounts are reset.</li> </ul>	<ul style="list-style-type: none"> <li>🔥 <b>Confidentiality:</b> Private information available publicly.</li> <li>🔥 <b>Integrity:</b> Modification or deletion of data from an unauthorized party.</li> <li>🔥 <b>Availability:</b> Unable to update or access the environment until it is secured and accounts are reset.</li> </ul>
---	--



Intel 471 has also observed the group follow TTPs in the MDCoA column, but then leverage the credentials in secondary or tertiary attacks. Additionally, the group will also search a company's GitHub repository source code for vulnerabilities within the code itself. These vulnerabilities are used in further, more complex, third-party or supply chain attacks.

ShinyHunters may not have as much notoriety as the ransomware groups that are currently causing havoc for enterprises all over the world. However, tracking actors like this are crucial to preventing your enterprise from being hit with such an attack. The information ShinyHunters gathers is often turned around and sold on the same underground marketplaces where ransomware actors use it to launch their own attacks. If enterprises can move to detect activity like ShinyHunters, they in turn can stop ransomware attacks before they are ever launched.

## APPENDIX:

### MITRE ATT&CK Techniques

#### **Reconnaissance** [TA0043]

- Gather Victim Identity Information: Credentials [T1589.001] - Sold unauthorized access credentials containing PII.
- Gather Victim Identity Information: Email Addresses [T1589.002] - Sold unauthorized access credentials containing PII.
- Phishing for Information [T1598]. Conducted phishing attacks targeting Microsoft Office 365 corporate users to steal account credentials.

#### **Initial Access** [TA0001]

- Phishing [T1566] - Conducted phishing attacks targeting Microsoft Office 365 corporate users to steal account credentials.
- Valid Accounts: Domain Accounts [T1078.002], Sold unauthorized access credentials containing PII.
- Valid Accounts: Cloud Accounts [T1078.004]. Used AWS keys to obtain further access to cloud services and subsequently dumped databases hosted through AWS.

### **Credential Access** [TA0006]

Steal Application Access Tokens [T1528] - Leveraged stolen Amazon Web Services (AWS) keys.

### **Discovery** [TA0007]

Cloud Infrastructure Discovery [T1580] - Reset passwords for accounts with access to the victim organization's GitHub software repository system and sought Amazon Web Services (AWS) keys.

### **Lateral Movement** [TA0008]

- Exploitation of Remote Services [T1210] - Searched GitHub repository for OAuth keys and used them to move laterally to a cloud service.
- Software Deployment Tools [T1072] - Used GitHub repository.

### **Collection** [TA0009]

- Data from Cloud Storage Object [T1530] - Used AWS keys to obtain further access to cloud services and subsequently dumped databases hosted through AWS.
- Data from Information Repositories [T1213]. Searched GitHub repository for OAuth keys and used them to move laterally to a cloud service.

### **Exfiltration** [TA0010]

Exfiltration Over Web Service [T1567]. Searched GitHub repository for OAuth keys and used them to move laterally to a cloud service.