The average ransom demand for a REvil ransomware infection is a whopping $260,000

Security researchers sinkhole the REvil ransomware servers and gain an insight into the operation of today's biggest ransomware gang.

Honda global operations halted by ransomware attack

Zack Whittaker @zackwhittaker / 8:07 am MDT • June 9, 2020

Comment

Subscribe to RSS
Follow me on Twitter
Join me on Facebook

KrebsonSecurity

In-depth security news and investigation

ADVERTISING/SPEAKING | ABOUT THE AUTHOR

09 JUN 20 Florence, Ala. Hit By Ransomware 12 Days After Being Alerted by KrebsOnSecurity

In late May, KrebsOnSecurity alerted numerous officials in **Florence, Ala.** that their information technology systems had been infiltrated by hackers who specialize in deploying ransomware. Nevertheless, on Friday, June 5, the intruders sprang their attack, deploying ransomware and demanding nearly $300,000 worth of bitcoin. City officials now say they plan to pay the ransom demand, in hopes of keeping the personal data of their citizens off of the Internet.

Nestled in the northwest corner of Alabama, Florence is home to roughly 40,000 residents. It is part of a quad-city metropolitan area perhaps best known for the Muscle Shoals Sound Studio that recorded the dulcet tones of many big-name music acts in the 1960s and 70s.

Image: Florenceal.org

On May 26, acting on a tip from Milwaukee, Wisc.-based cybersecurity firm Hold Security, KrebsOnSecurity contacted the office of Florence's mayor to alert them that a Windows 10 system in their IT environment had been commandeered by a ransomware gang.

Comparing the information shared by Hold Security dark web specialist **Yuliana Bellini** with the employee directory on the Florence website indicated the username for the

FELIPE ERAZO 1 HOUR AGO

Ransomware Gangs Are Teaming Up to Form Cartel-Style Structures

The latest moves from ransomware groups suggest that gangs are forging alliances to create a mafia-style structure.

3258 Total views 45 Total shares Listen to article 2:32

User Training

- Look at how we currently handle vulnerability assessments
- Regular and scheduled tests of technical assets
- We need to do the same with people
- Regular testing
- The 20% rule
  - But! Who is consistently in the 20%?
  - Address these people with additional training
- Reward people who spot the tests, and real attacks
- Lets talk of %

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

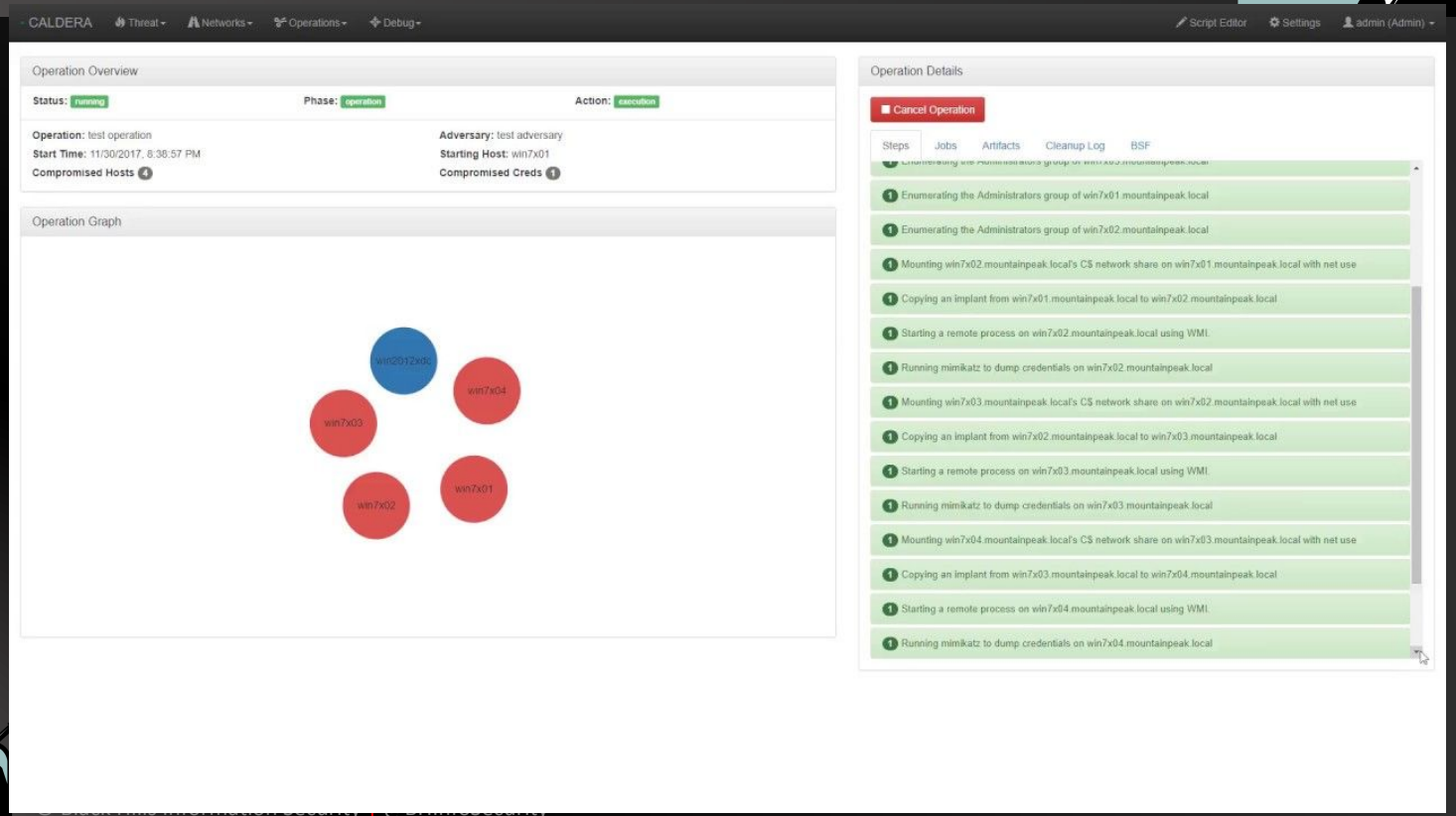
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding

https://attack.mitre.org/

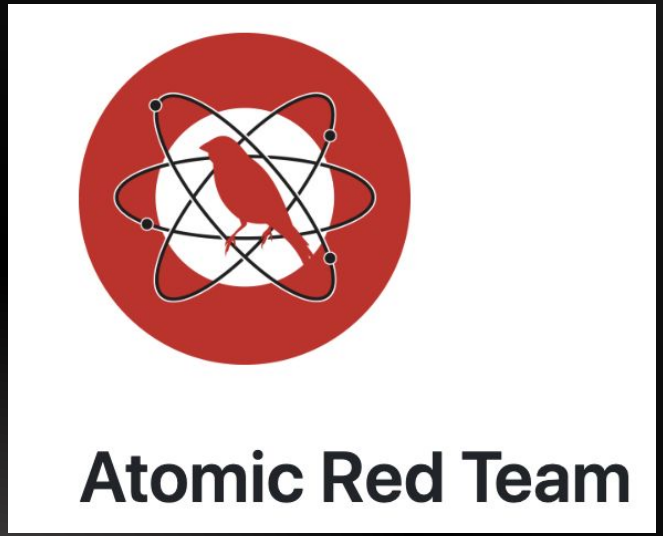
But, We Should Be Emulating

- A lot…
- Like all the time
- With many, many different tools
- Believe it or not, this is Threat Intel
- Using tools and hiring testers is applied threat intelligence
  - But it requires repetition and understanding of the attacks
- It gives you the ability to see how your organization will react to a *dynamic* attack

Open Source Tool Example: Caldera



Open Source Tool Example: Atomic Red Team



Execute All Attacks for a Given Technique

```
Invoke-AtomicTest T1117
```

Speficy a Process Timeout

```
Invoke-AtomicTest T1117 -TimeoutSeconds 15
```

If the attack commands do not exit (return) within in the specified `-TimeoutSeconds`, the process and it's children will be forcefully terminated. The default value of `-TimeoutSeconds` is 120. This allows the `Invoke-AtomicTest` script to move on to the next test.

Execute All Tests

This is not recommended but you can execute all Atomic tests in your atomics folder with the follwing:

```
Invoke-AtomicTest All
```

Execute All Tests from a Specific Directory

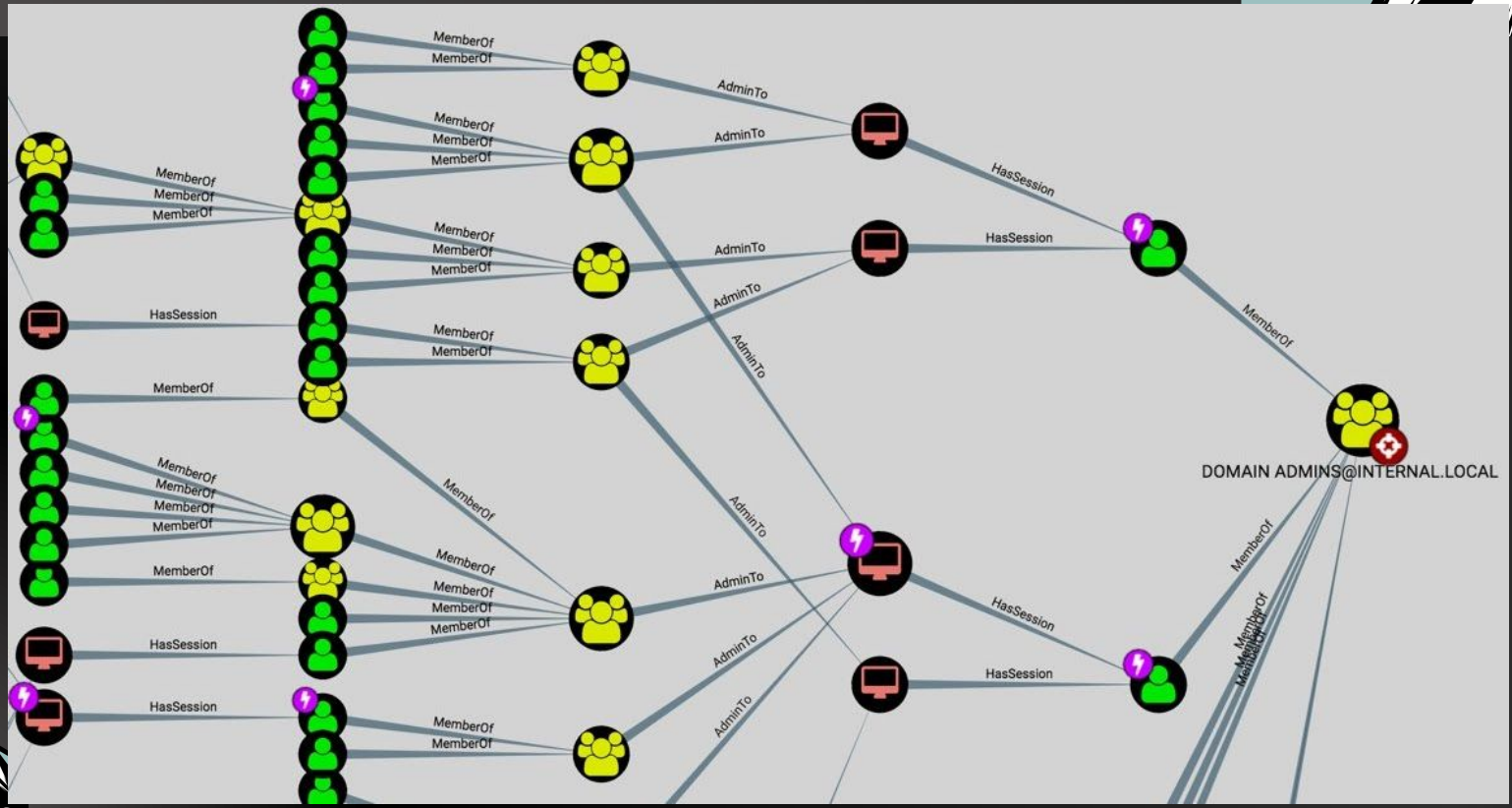
Specify a custom path to your atomics folder, example C:\AtomicRedTeam\atomics

```
Invoke-AtomicTest All -PathToAtomicsFolder C:\AtomicRedTeam\atomics
```

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1117 -TestNumbers 1 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Regsvr32 T1117
Atomic Test Name: Regsvr32 local COM scriptlet execution
Atomic Test Number: 1
Description: Regsvr32.exe is a command-line program used to register and unregister OLE controls.
Upon execution, calc.exe will be launched.
Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
regsvr32.exe /s /u /i:#{filename} scrobj.dll
Command (with inputs):
regsvr32.exe /s /u /i:C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct scrobj.dll
Dependencies:
Description: Regsvr32.exe must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1117
\src\RegSvr32.sct)
Check Prereq Command:
if (Test-Path #{filename}) {exit 0} else {exit 1}
Check Prereq Command (with inputs):
if (Test-Path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) {exit 0} else {exit 1}
Get Prereq Command:
New-Item -Type Directory (split-path #{filename}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "#{filename}"
Get Prereq Command (with inputs):
New-Item -Type Directory (split-path C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct) -ErrorAction
 ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/Reg
Svr32.sct" -OutFile "C:\AtomicRedTeam\atomics\T1117\src\RegSvr32.sct"
[!!!!!!!!END TEST!!!!!!!]
```

Open Source Tool Example: Bloodhound



Threat Emulation Warning

- One of the traps of the MITRE framework and threat emulation is we train or systems to detect specific attacks
- Most of the attacks in Atomic Red Team and MITRE are representations of classes of attacks
- We are seeing vendors simply detect those attacks
  - More on this later!
- A few modifications and you can easily bypass detection

Commercial Offerings

ATTACKIQ

SCYTHE

XM CYBER

PlumHound

README.md

PlumHound - BloodHoundAD Report Engine for Security Teams

Released as Proof of Concept for Blue and Purple teams to more effectively use BloodHoundAD in continual security life-cycles by utilizing the BloodHoundAD pathfinding engine to identify Active Directory security vulnerabilities resulting from business operations, procedures, policies and legacy service operations.

PlumHound operates by wrapping BloodHoundAD's powerhouse graphical Neo4J backend cypher queries into operations-consumable reports. Analyzing the output of PlumHound can steer security teams in identifying and hardening common Active Directory configuration vulnerabilities and oversights.

Checks

```
python3 PlumHound.py -x tasks/default.tasks

[*]Building Task List
[*]Beginning Output HTML:reports\DomainUsers.html
[*]Beginning Output HTML:reports\Keroastable_Users.html
[*]Beginning Output HTML:reports\Workstations_RDP.html
[*]Beginning Output HTML:reports\Workstations_UnconstrainedDelegation.html
[*]Beginning Output HTML:reports\GPOs.html
[*]Beginning Output HTML:reports\AdminGroups.html
[*]Beginning Output HTML:reports\ShortestPathDA.html
[*]Beginning Output HTML:reports\RDPableGroups.html
[*]Beginning Output HTML:reports\Groups_CanResetPasswords.html
[*]Beginning Output HTML:reports\LocalAdmin_Groups.html
[*]Beginning Output HTML:reports\LocalAdmin_Users.html
[*]Beginning Output HTML:reports\DA_Sessions.html
[*]Beginning Output HTML:reports\Keroastable_Users_MostPriv.html
[*]Beginning Output HTML:reports\OUs_Count.html
[*]Beginning Output HTML:reports\Permissions_Everyone.html
[*]Beginning Output HTML:reports\Groups_MostAdminPriviledged.html
[*]Beginning Output HTML:reports\Computers_WithDescriptions.html
[*]Beginning Output HTML:reports\Users_NoKerbReq.html
[*]Beginning Output HTML:reports\Users_Count_DirectAdminComputers.html
[*]Beginning Output HTML:reports\Users_Count_InDirectAdminComputers.html
[*]Beginning Output HTML:reports\Users_NeverActive_Enabled.html
```

PlumHound

User to Local Admin Count:

COMPUTER	USER
1	TERRY_HARPER@WLABV3.LOCAL
1	ADMINISTRATOR@WLABV3.LOCAL
1	IMOGENE_KELLEY@WLABV3.LOCAL

OU to Object Count:

o.name	o.guid	COUNT(c)
TEST@WLABV3.LOCAL		13
SERVICEACCOUNTS@WLABV3.LOCAL		11
GROUPS@WLABV3.LOCAL		7
DEVICES@WLABV3.LOCAL		6
TIER 1@WLABV3.LOCAL		4
T0-ACCOUNTS@WLABV3.LOCAL		2
SECFRAME.COM@WLABV3.LOCAL		2
FIN@WLABV3.LOCAL		2
GOO@WLABV3.LOCAL		2
T1-ACCOUNTS@WLABV3.LOCAL		1
T2-DEVICES@WLABV3.LOCAL		1
T2-ROLES@WLABV3.LOCAL		1
T2-SERVERS@WLABV3.LOCAL		1
AZR@WLABV3.LOCAL		1
ADMIN@WLABV3.LOCAL		1
AWS@WLABV3.LOCAL		1
DOMAIN CONTROLLERS@WLABV3.LOCAL		1
BDE@WLABV3.LOCAL		1
SEC@WLABV3.LOCAL		1
QUARANTINE@WLABV3.LOCAL		1

Indirect User to Local Admin Computer

m.name	n.name
ADMINISTRATOR@WLABV3.LOCAL	DC01.WLABV3.LOCAL
IMOGENE_KELLEY@WLABV3.LOCAL	DC01.WLABV3.LOCAL
TERRY_HARPER@WLABV3.LOCAL	DC01.WLABV3.LOCAL

Local Admin Groups (groups found in LA)

m.name	n.name
DOMAIN ADMINS@WLABV3.LOCAL	DC01.WLABV3.LOCAL
ENTERPRISE ADMINS@WLABV3.LOCAL	DC01.WLABV3.LOCAL

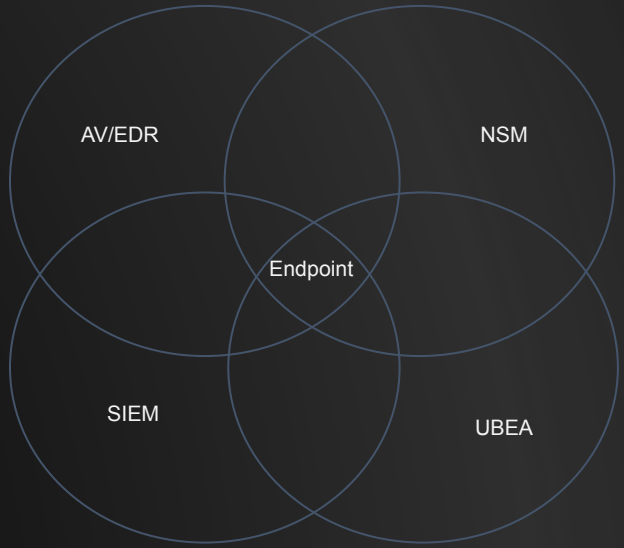
Group to Count of Admin Rights (LA/DA)

GroupName	AdminRightCount
ENTERPRISE ADMINS@WLABV3.LOCAL	1
DOMAIN ADMINS@WLABV3.LOCAL	1

n.name	n.displayname	n.description	n.title	n.pwdneverexpires	n.passwordnotreqd	n.sensitive	n.admincount	n.serviceprincipalnames
KRBTGT@WLABV3.LOCAL		Key Distribution Center Service Account		False	False	False	True	['kadmin/changepw']

Don't Focus On Just One Product

- The key is overlapping fields of visibility
- Endpoint
- SIEM/UBEA
- Network Monitoring
- Sandboxing
- Internal Segmentation



Paying

- If you pay, you can negotiate
- Sometimes, for more than 50% off
- A couple of tactics
  - Don't contact as your own company
  - Contact as a consulting firm
  - Negotiate your cost minus the cost of the payout
- All the above is "bad" advice

Takeaways… Go back to work and..

- Check backups and ask, “how could an attacker break this?”
- Revisit user awareness training
- Test principle of least privilege
- Enable workstation firewalls
- Talk about paying and not paying with management
- Start emulating attackers… Now.

Questions?