Controlware Security Day 2022

Conti-Ransomware auf dem Operationstisch

Chris Trynoga
Senior Security Engineer
ctrynoga@akamai.com

Conti-Ransomware auf dem Operationstisch

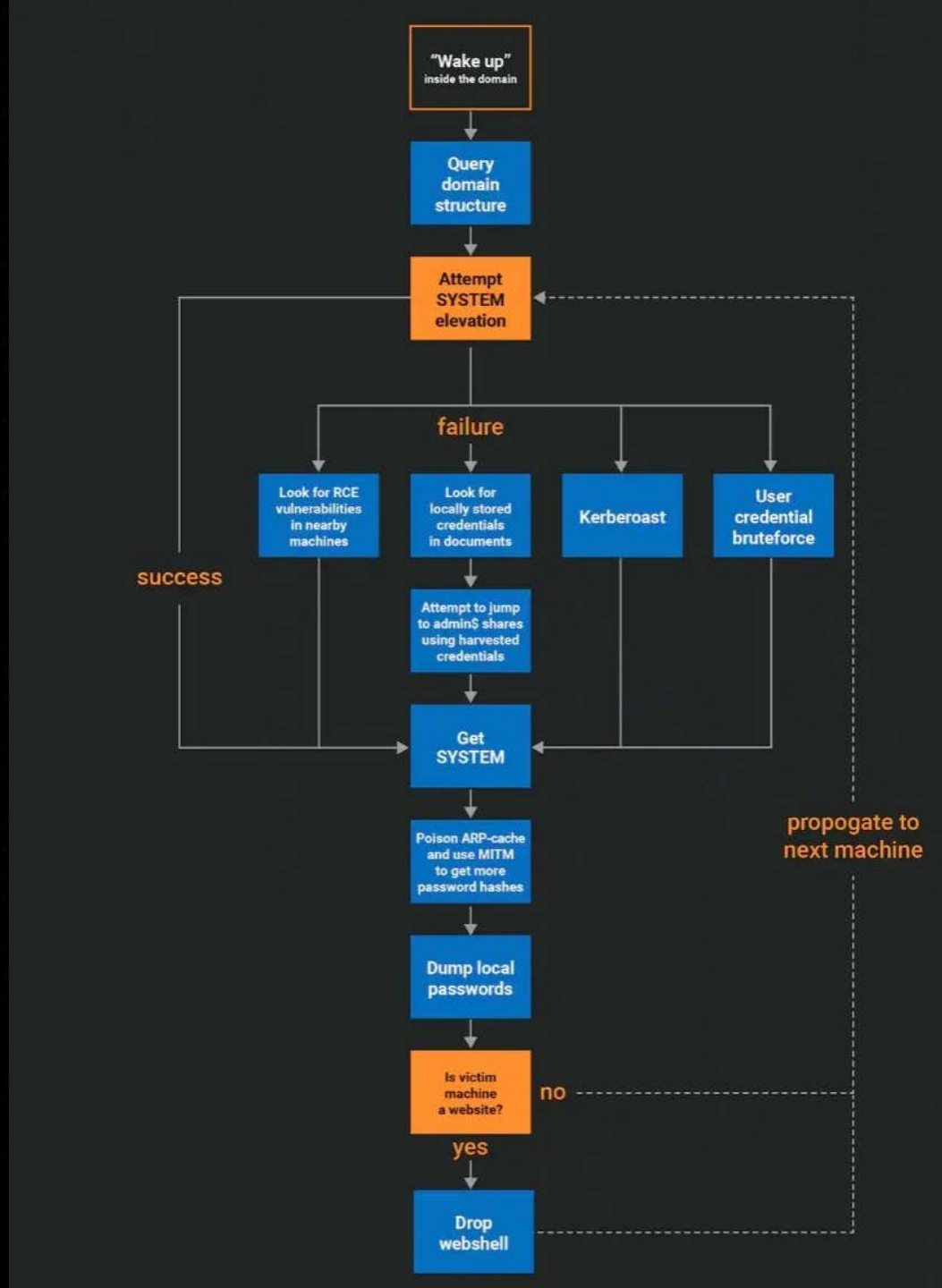
Chris Trynoga
Senior Security Engineer
18.05.2022

Conti and the Hacker's Manual

Conti is a ransomware gang with revenues projected at almost $200M.

On February 27, 2022, the Twitter handle @contileaks began leaking internal documents and chat logs of the group, as well as the addresses of some of their internal servers and source code.

Akamai researchers analyzed this and published their "Hacker's Manual"



A useful framework for articulating modern attacks.

Tactics: The adversary's tactical goal: the reason for performing an action.

Techniques: The means by which an adversary achieves a tactical goal.

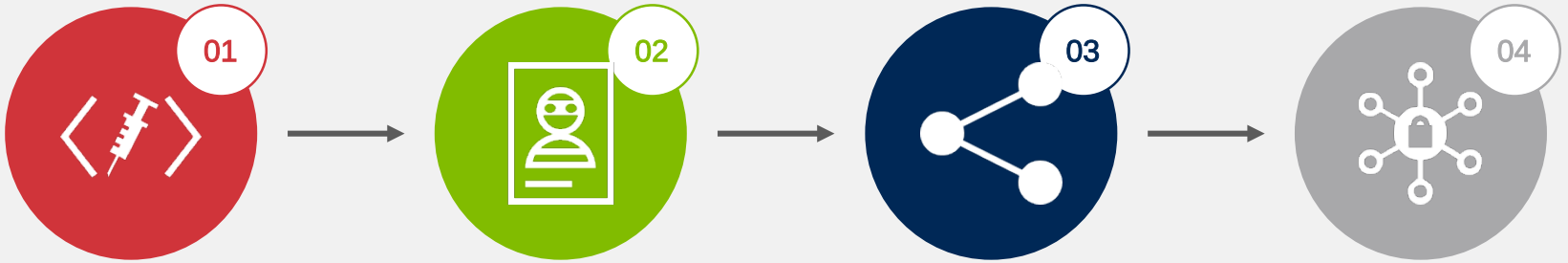
controlware Akamai

Simplified Attack Chain

Key Phases

Tactics

Ransomware does not begin and end with encryption. Multiple adversarial tactics precede disaster.



Initial Access
Achieve an initial foothold (not usually lucrative target)

Privilege Escalation
Gain administrative privileges

Lateral Movement
Spread to large portion of network or target assets

Impact
Mass encryption, exfiltration

Techniques

Conti has an arsenal of techniques to enable their tactics to succeed depending on the circumstances.

Outlook Web Access, RDP, SQL, Printers, Apache Tomcat Scanner, Mail

PrintNightmare, Mimikatz

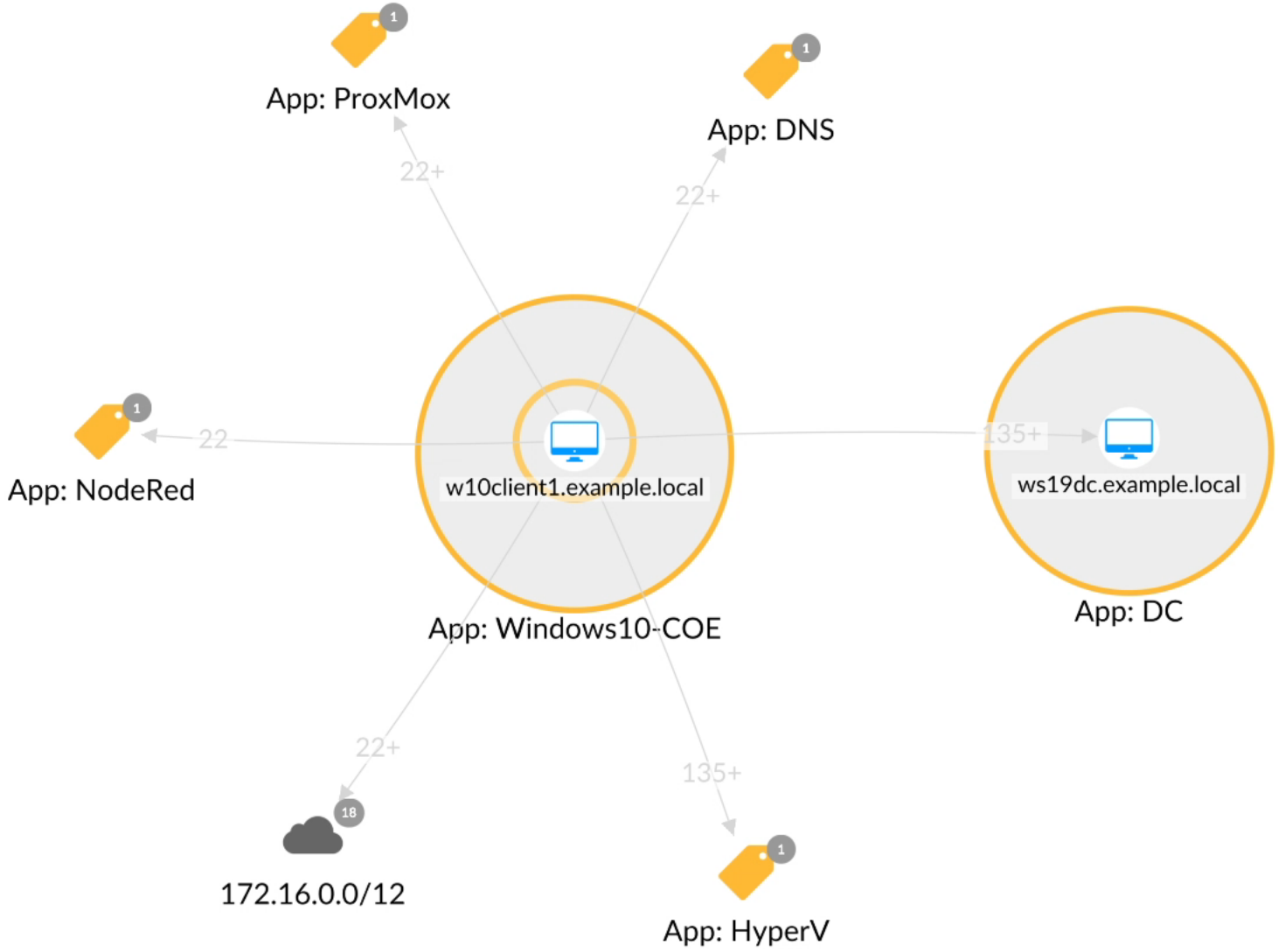
PSExec, WMI, Remote Task Scheduler, WinRM, BlueKeep, EternalBlue

Data encrypted for impact, Exfiltration over alternative protocol

controlware Akamai

Live Demo

Map: Unfiltered map | Group By: App | 2022-08-03 20:09 - 21:09 | Highlight by name



w10client1.example.local (On)

Information

From installed agent (Download Policy)

Name	w10client1.example.local
OS	Windows *Microsoft Windows 10 Enterprise* *6.2* *Version 6.2*
CPUs	1 *Architecture: amd64*
Agent Version	5.42.22098.12204
IP Addresses	172.27.7.202 fe80::4cdd:af55:a6d8:789f
MAC Addresses	00:15:5d:07:04:0c

Labels

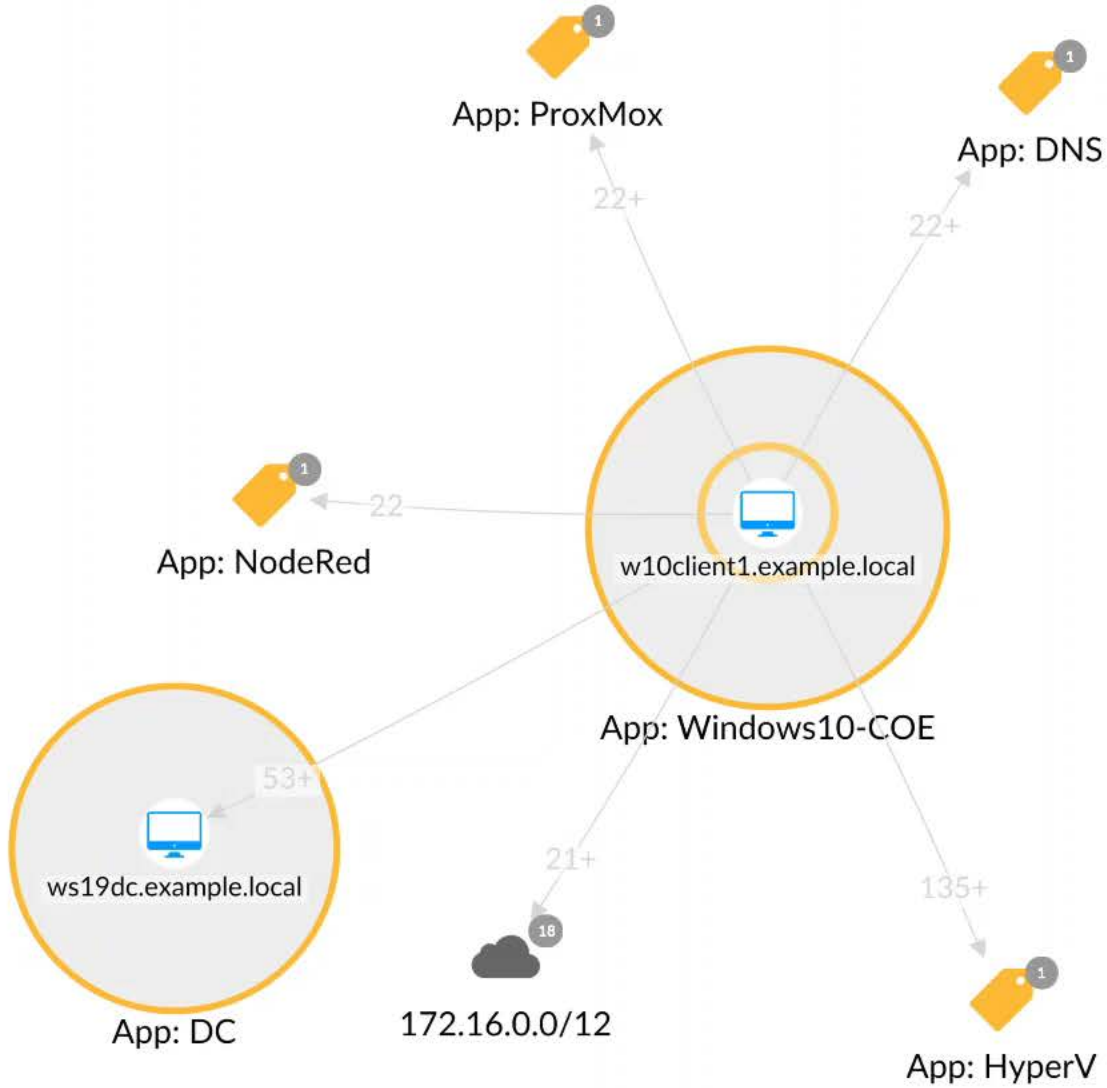
Key | Value

Add

Segmentation Policy | Related Incidents | DNS Requests

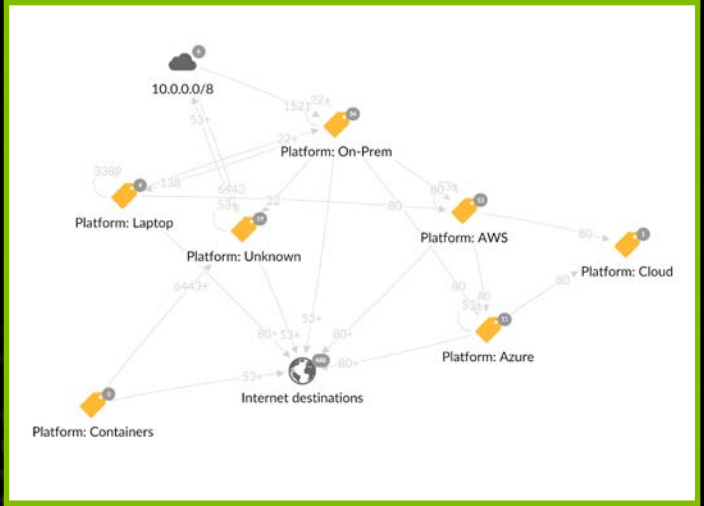
Source	Request	Response	Arrival Time
172.27.7.202	fp.msedge.net	204.79.197.222	2022-08-03 21:04:34
172.27.7.202	fp-vp.azureedge.net	152.199.19.161	2022-08-03 21:04:34
172.27.7.202	t-ring.msedge.net	13.107.246.254	2022-08-03 21:04:34
172.27.7.202	www.bing.com	204.79.197.200	2022-08-03 21:04:26
172.27.7.202	ws19dc.example.local	172.27.7.200	2022-08-03 21:04:17
172.27.7.202	array507.prod.do.dsp.mp.microsoft.com	52.184.217.20	2022-08-03 21:03:17
172.27.7.202	www.bing.com	204.79.197.200	2022-08-03 21:02:57
172.27.7.202	checkappexec.microsoft.com	20.67.219.150	2022-08-03 21:02:37
172.27.7.202	ws19dc.example.local	172.27.7.200	2022-08-03 21:02:25
172.27.7.202	download.sysinternals.com	152.199.19.160	2022-08-03 21:02:25
172.27.7.202	ctldl.windowsupdate.com	13.107.4.50	2022-08-03 21:02:13
172.27.7.202	raw.githubusercontent.com	185.199.108.133	2022-08-03 21:01:44
172.27.7.202	github.com	140.82.121.3	2022-08-03 21:01:43
172.27.7.202	ws19dc.example.local	172.27.7.200	2022-08-03 21:01:40

Map: Unfiltered map | Group By: App | 2022-08-03 20:09 - 21:09 | Highlight by name

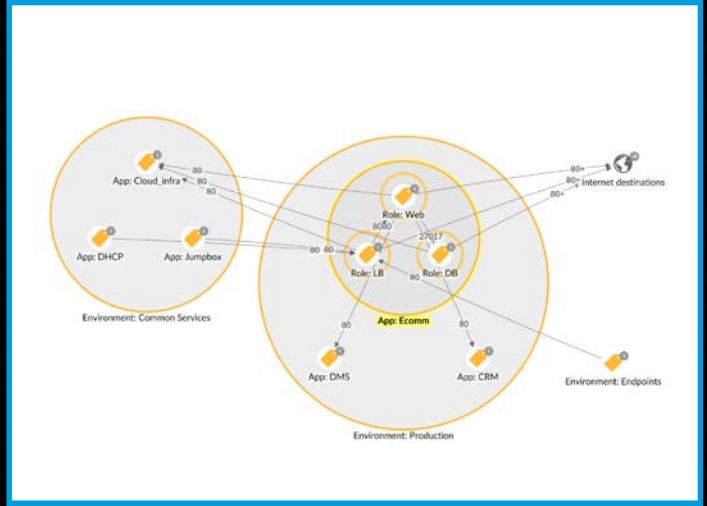


Our Approach to Microsegmentation

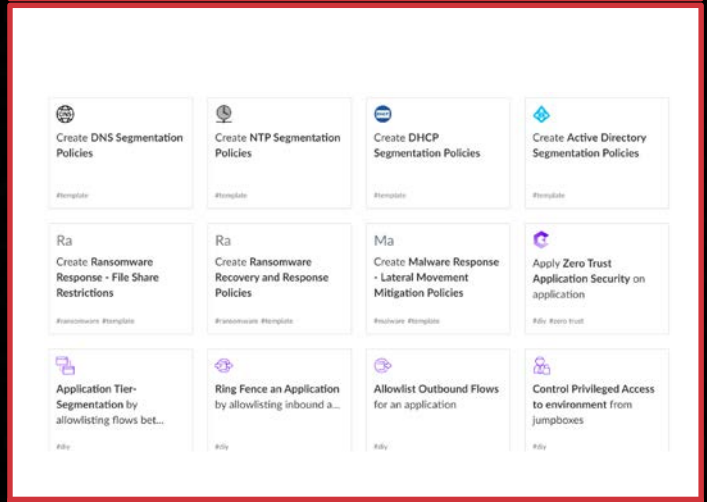
Visualization



Mapping

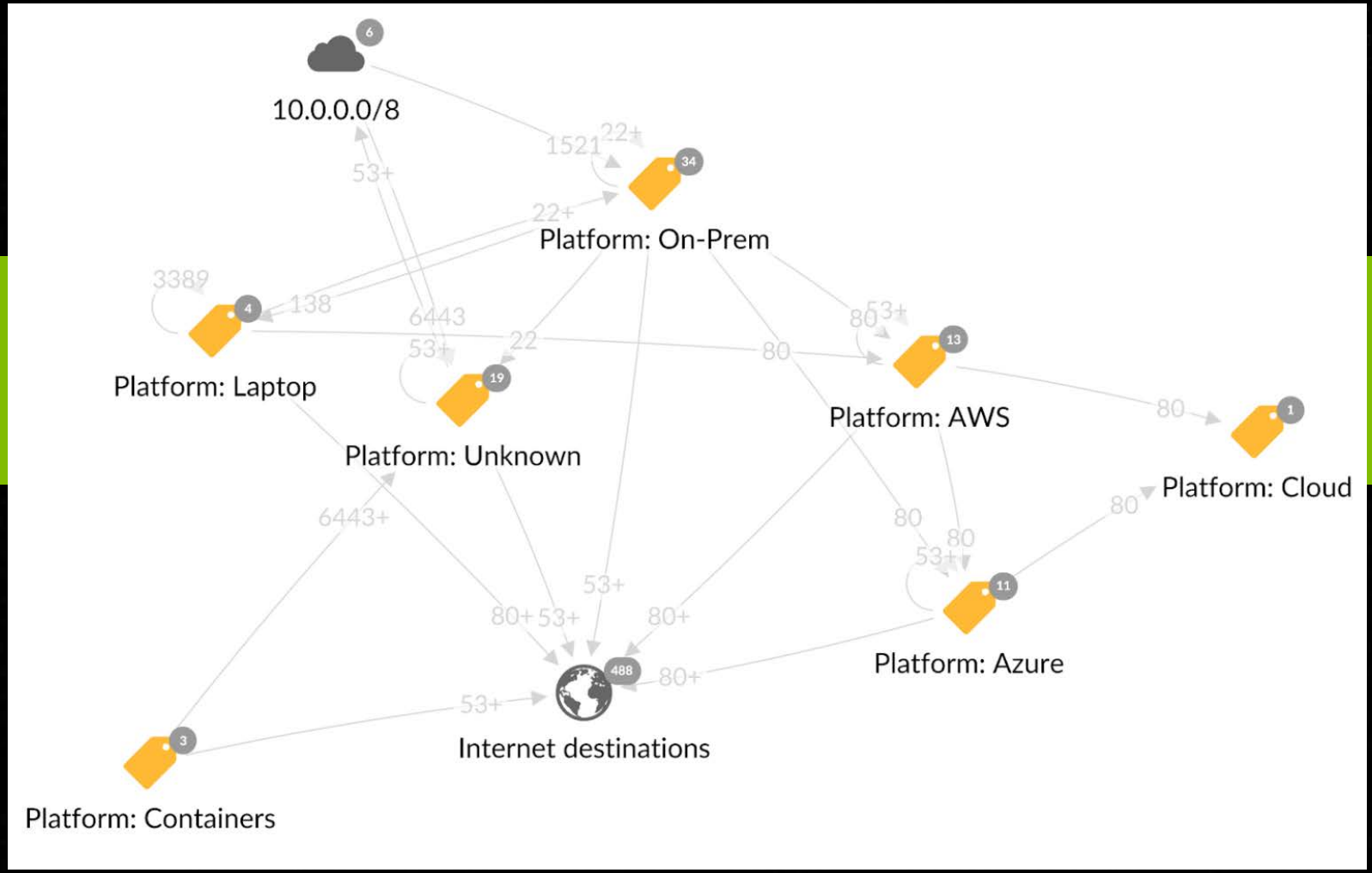


Policy



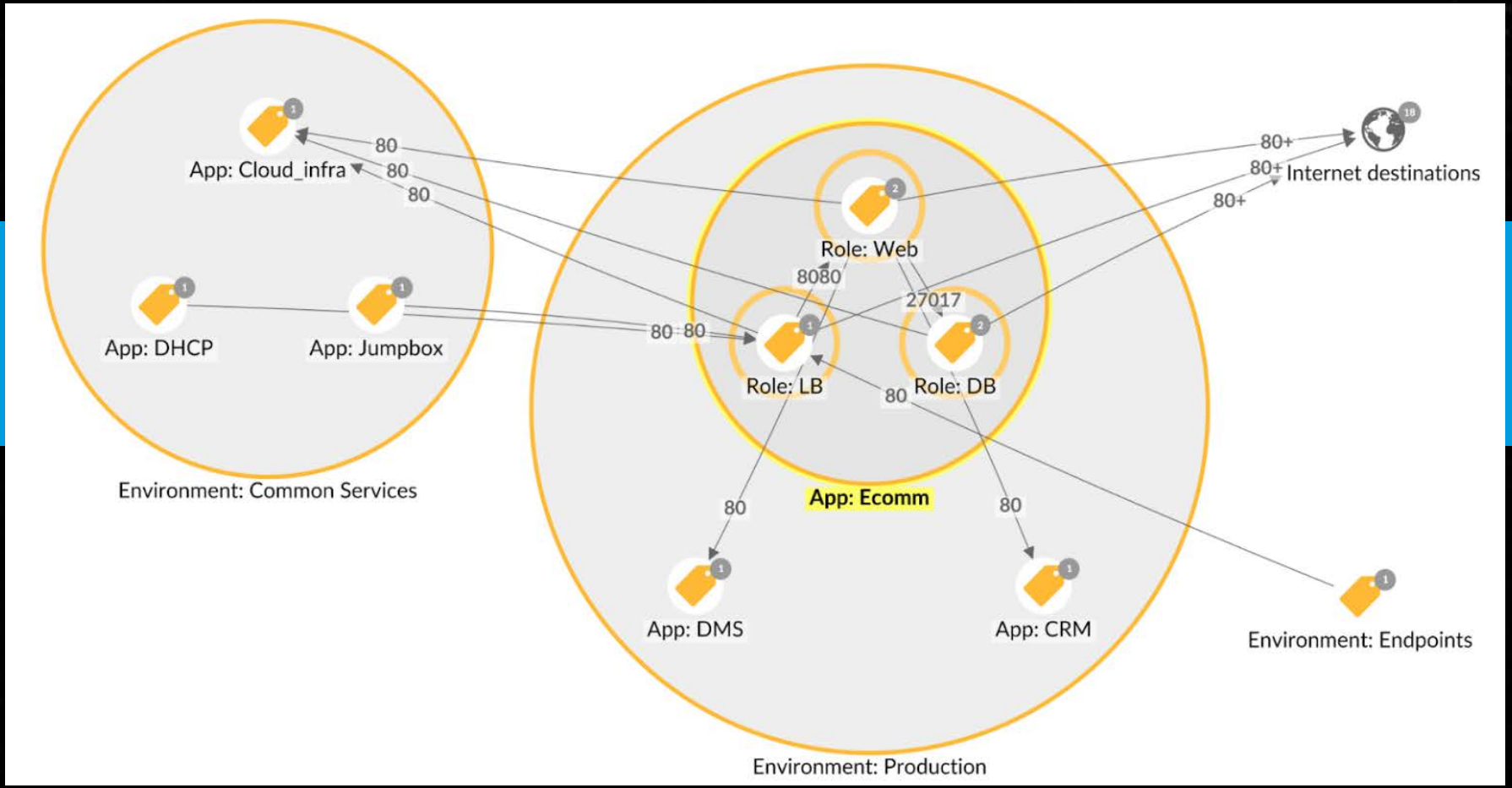
Our Approach to Microsegmentation

Visualization



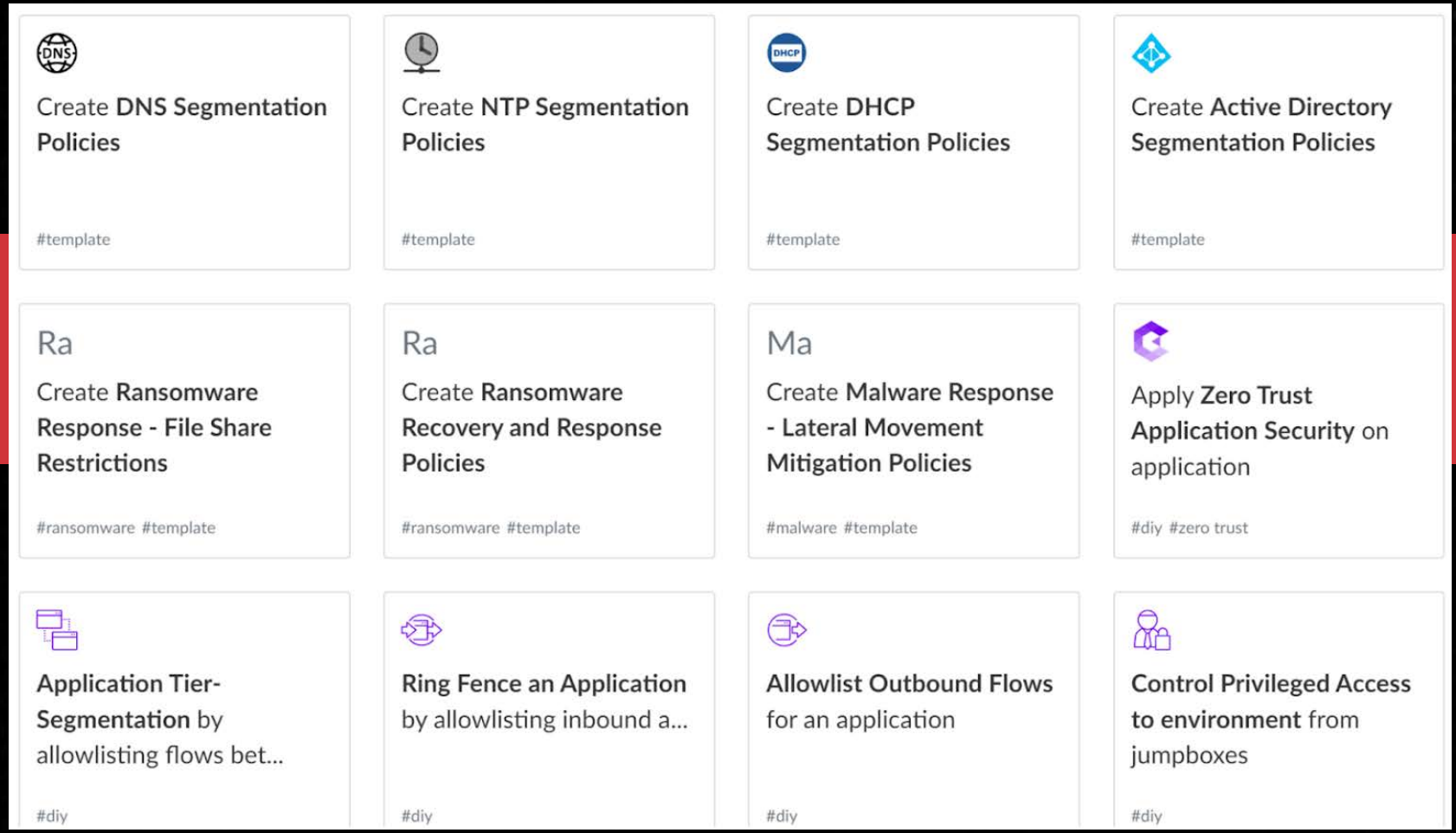
Our Approach to Microsegmentation

Mapping

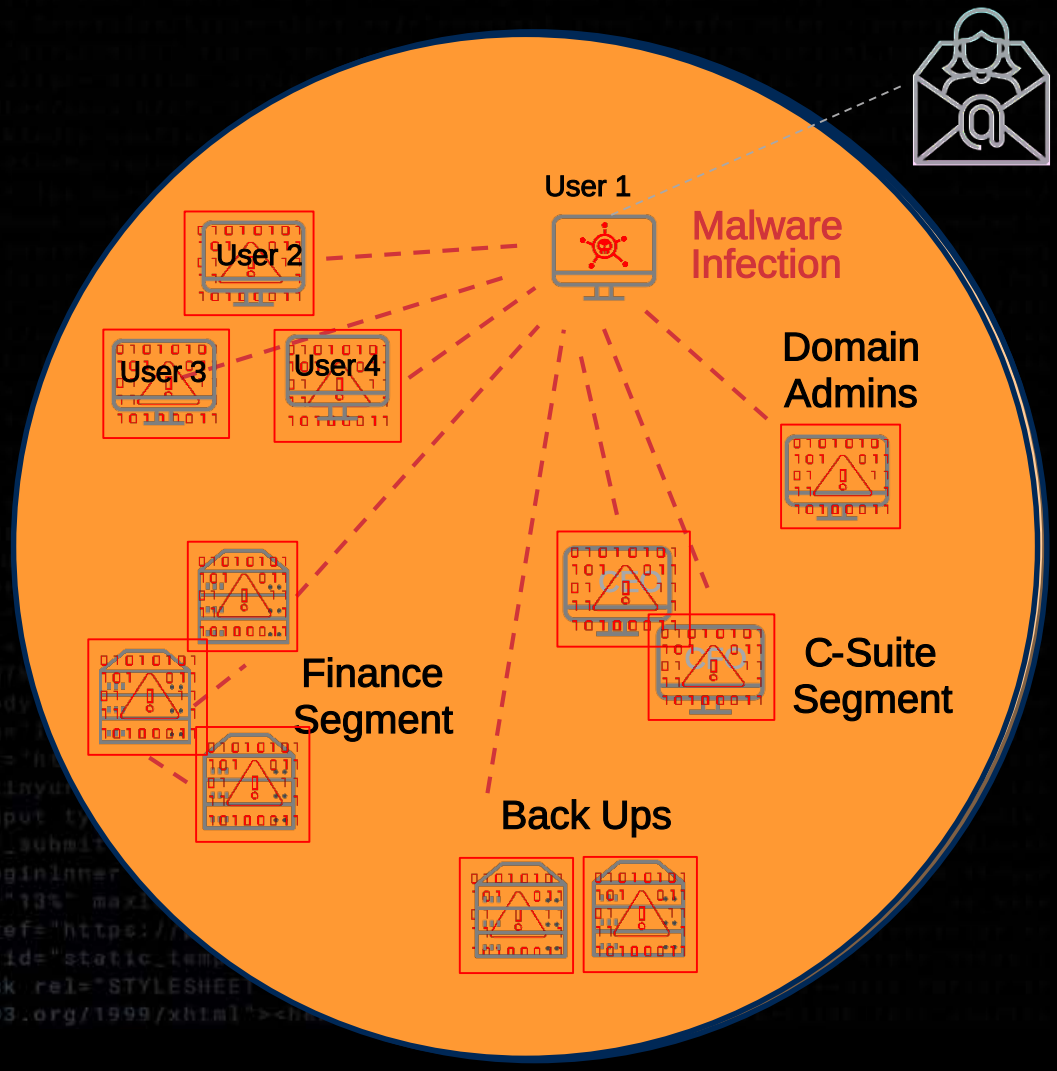


Our Approach to Microsegmentation

Policy



Ransomware *without* Segmentation

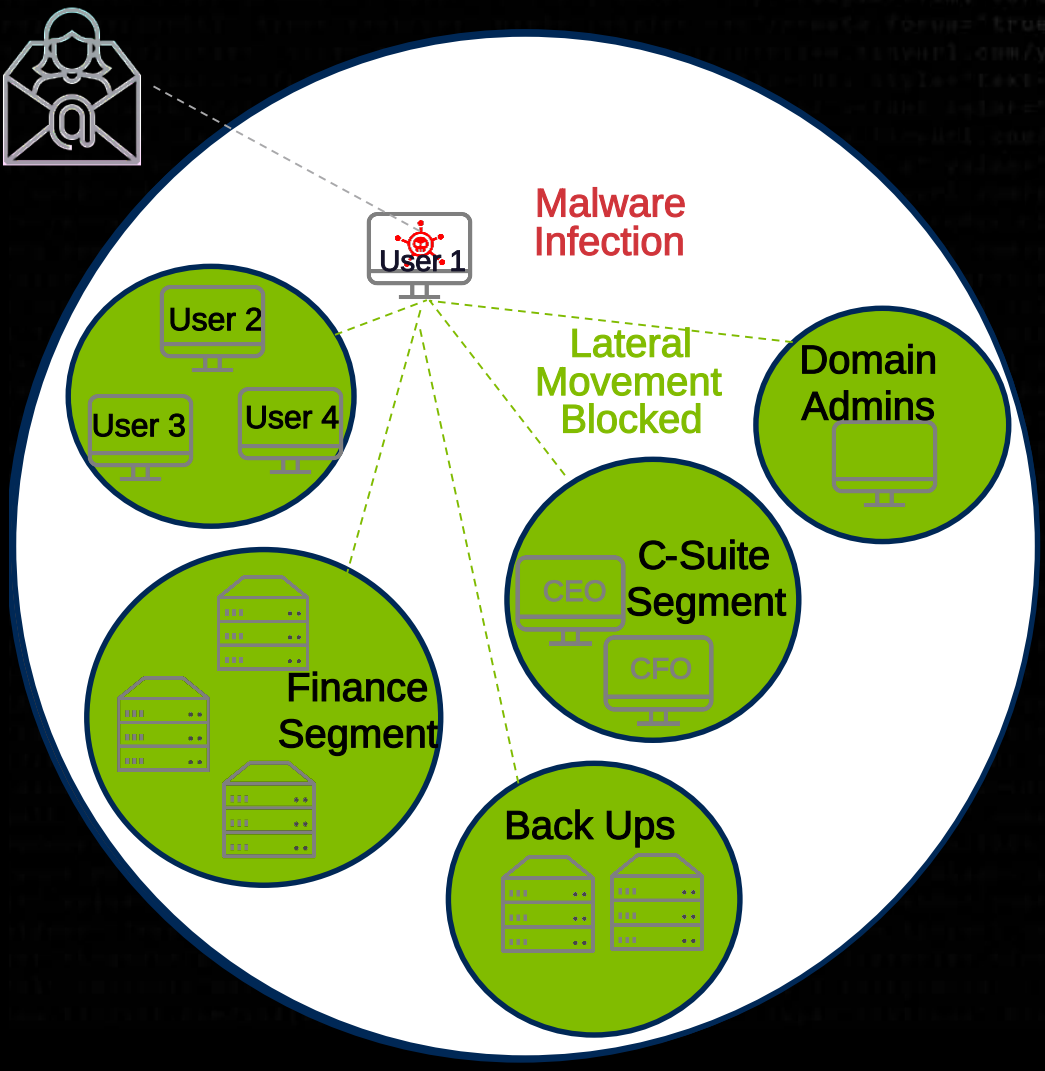


1. User clicks phishing email

2. Attackers begin intelligence gathering

3. Attackers drop ransomware

Ransomware *with* Segmentation



Recommendations

1

Analyze The Threat (Hacker's Manual)

2

Know Your Defenses (Defender's Manual)

2

Fill in the Gaps (ATT&CK Navigator)

Thank You

Zeit für eine Testfahrt?