CISA Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector

On Oct 28, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) along with the Federal Bureau of Investigations (FBI) and Health and Human Services (HHS) announced of an increased and imminent cyberthreat to the Healthcare and Public Health Sector. This warning comes on the heels of increased ransomware incidents in the last few months and includes information on Conti, TrickBot, BazarLoader and new Indicators of Compromise (IOCs). As healthcare continues to grow as a reliable source of income for threat actors because of the necessity to **protect patient care**, ransomware campaigns will continue to proliferate.

Jeff Horne, Chief Security Officer at Ordr, provides insight into the latest wave of ransomware with a series of articles:

- **Ransomware in Healthcare Providers and Healthcare Delivery Organizations—Tactics, Techniques, and Procedures and Recommendations of How to Triage**
- **A Primer on Preparing for and Responding to Ransomware for Users of IoT and IoMT**
- **Ordr CISO Threatcast – Ransomware Affecting Healthcare**

Threat Summary

Ransomware has been around for decades and while the recent evolution in the past few years has transformed into more of a service – yes, Ransomware-as-a-Service (RaaS), it can be attributed to one of the reasons there is a **25 percent increase in attacks from Q4 2019 to Q1 2020 and a 715% year-over-year increase in detected—and blocked—ransomware attacks** and the **average payment increased by 33%**.

The distributed nature of the ransomware developer and the affiliates makes it more lethal than ever. How RaaS works is explained in simple diagram below:

Ransomware developer: Who creates custom malicious code, and capabilities like lateral movement tools and scripts, and including exploit code that is sold to a ransomware affiliate for a fee or share in eventual ransom after a successful attack.

Ransomware affiliate: Starts a hosting site with custom exploit code. Identify targets and send the exploit code typically by phishing email or as an attachment.

Victim: Falls victim to the exploit code.

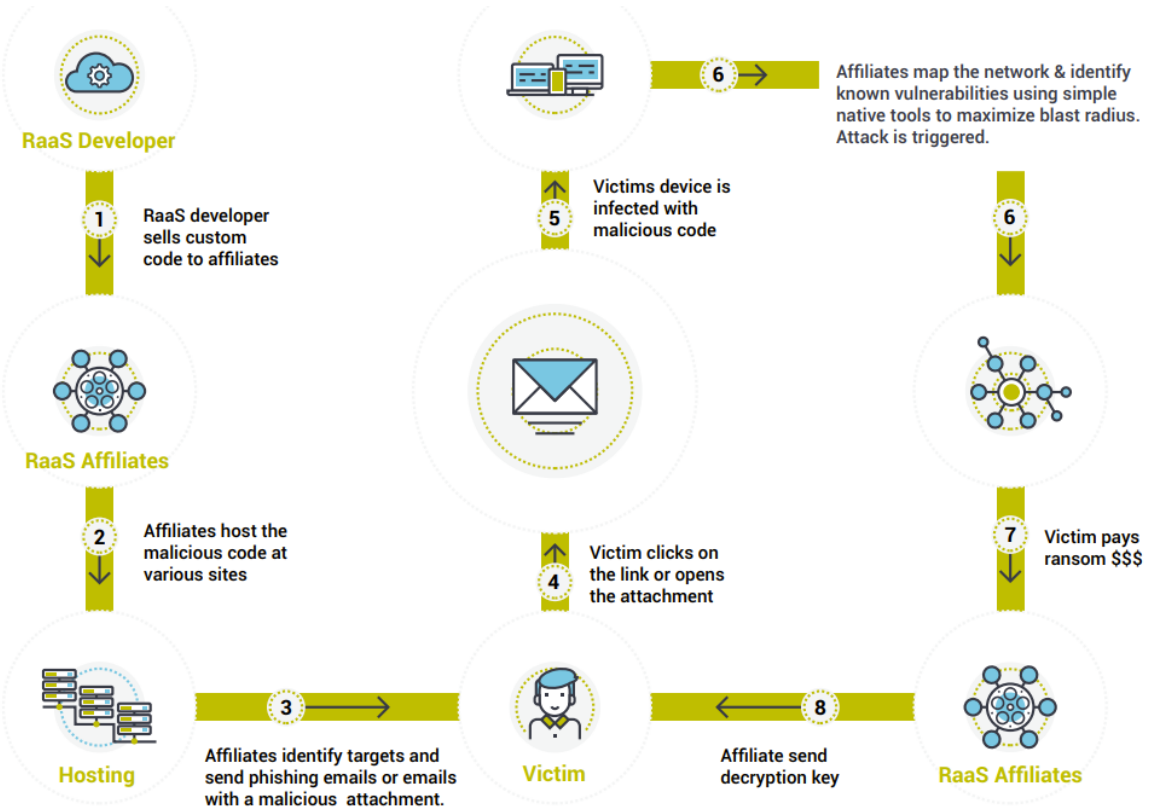


Figure 1: RaaS Infection Lifecycle

There are several RaaS types identified by security experts. Some examples are Sodinokibi, Ryuk, Mamba, Phobos, Dharma, Snatch, etc. It is worth noting that in the actual ransomware code is usually the last piece dropped in the infection life cycle giving hope that this can be prevented. The infection usually starts with Trojans like Trickbot, will go through the baking process where the RaaS affiliates monitor and map out the network and any existing vulnerabilities and then drop the actual ransomware code.

Using Ordr in defense against the recent Ransomware attacks

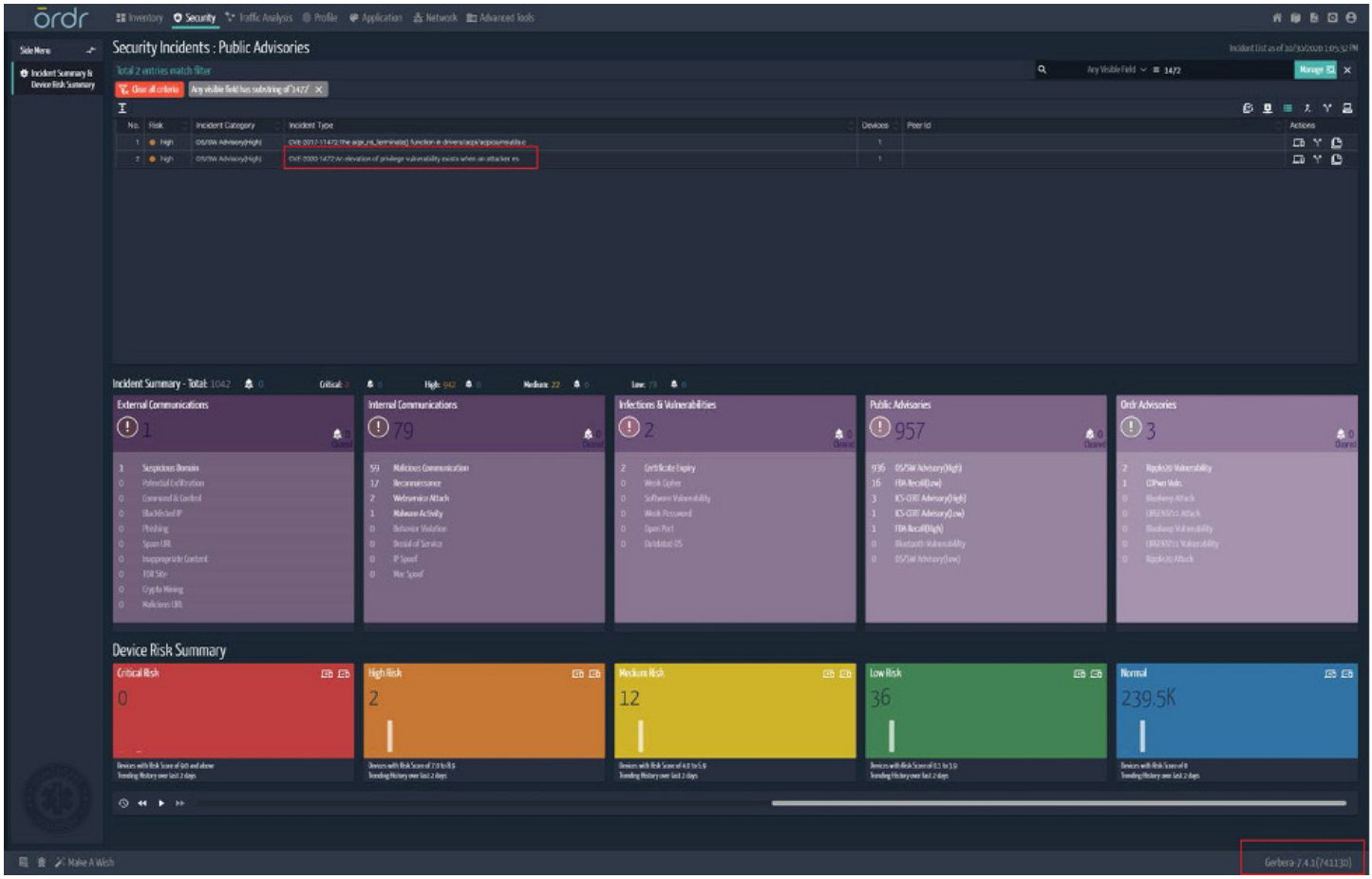
Ordr has been working on enhancing features and work with the industry partners to make it easy for customers to identify, detect and respond on any potential vulnerability and threats. Identifying vulnerabilities and active threats are both important in the fight against ransomware but they need to be handled differently. Vulnerability remediation needs good planning and execution whereas active threat is something that need to be addressed right away. Ordr addresses both vulnerability and active threat detection for the CISA AA20-302A advisory.

Vulnerability management with Ordr

Identify vulnerable devices:

One of the vulnerabilities the recent Ransomware seem to exploit is CVE-2020-1472 [7] termed ZeroLogon. ZeroLogon is a privilege escalation vulnerability which when exploited can quickly spread ransomware to the entire domain managed devices and services.

Ordr vulnerability databases are constantly updated and tags devices that are vulnerable to ZeroLogon vulnerability automatically. Making sure devices associated to these vulnerabilities are patched is the first defense towards ransomware attacks.



Make sure Anti-virus is installed on all workstations including virtual machines:

Ordr provides a quick and easy way to identify anti-virus status for all physical and virtual machines. Ordr has helped identify virtual machines running without any anti-virus software on numerous occasions. Make sure anti-virus is running on all physical and virtual machines and the definitions are updated.

No.	Mac Address	IP Address	Device Name	AntiVirus SW
8	A4:8C:DB:79:1B:71	10.51.159.238	DEMO-WINRM-ltaylor.ordrlab.c	
9	00:68:EB:7D:9B:C4	10.51.161.233	cwike.ordrlab.cpn.com	
10	08:2E:5F:7C:EE:39	10.51.156.63	jperry.ordrlab.cpn.com	
11	A4:8C:DB:79:29:75	10.51.160.72	User thinkpad-1	YES
12	00:19:0F:7C:5E:B7	10.51.156.97	jclark.ordrlab.cpn.com	
13	A4:8C:DB:79:6A:48	10.51.159.240	User thinkpad-2	YES
14	A4:8C:DB:7D:ED:27	10.51.159.229	User thinkpad-3	YES
15	A4:8C:DB:7F:26:24	10.51.160.29	User thinkpad-4	YES
16	A4:8C:DB:7A:4A:82	10.51.160.18	User thinkpad-5	YES
17	00:68:EB:78:A4:60	10.51.161.213	npace.ordrlab.cpn.com	YES
18	08:2E:5F:78:AB:1A	10.51.178.96	cwelborn.ordrlab.cpn.com	YES
19	B8:CA:3A:78:C6:7E	10.51.160.237	gperez.ordrlab.cpn.com	YES
20	A4:8C:DB:7F:26:A4	10.51.160.2	User thinkpad-6	YES

Third Party Software (87)

No.	Name	Vendor	Version	Installed On
3	Adobe Flash Player 30 ActiveX	Adobe Systems Incorporated	30.0.0.134	-
4	Adobe Refresh Manager	Adobe Systems Incorporated	1.8.0	Sat Sep 26 2020
5	Atellicar Inventory Manager v1.0.4	Siemens Healthineers	1.0.4.4	Wed Oct 23 2019
6	Cb Defense Sensor 64-bit	Carbon Black, Inc.	3.4.0.1097	Fri [redacted] 13 2019
7	Dell SupportAssist	Dell Inc.	3.5.0.448	Tue May 05 2020

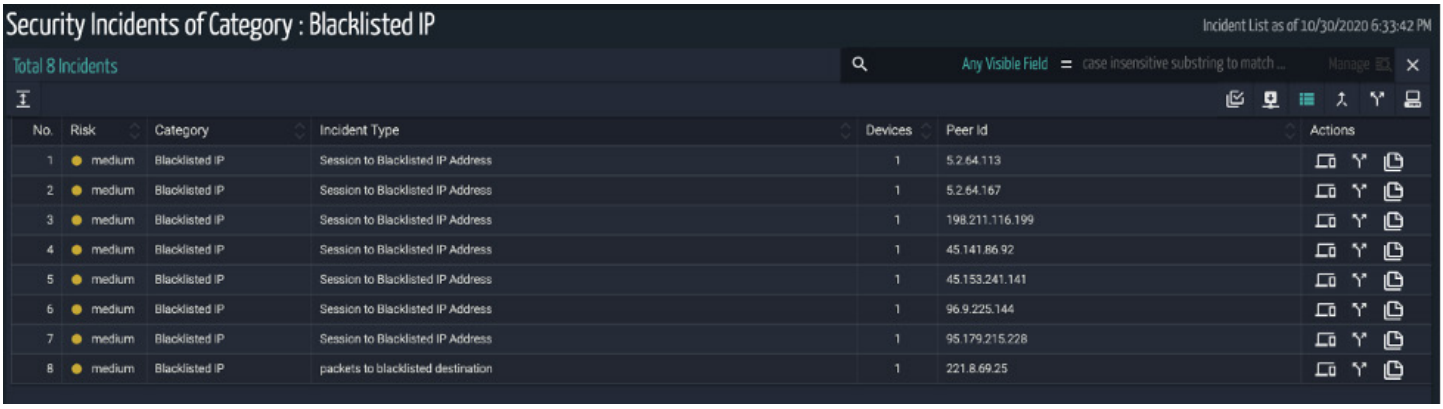
Identify and secure non-domain managed devices:

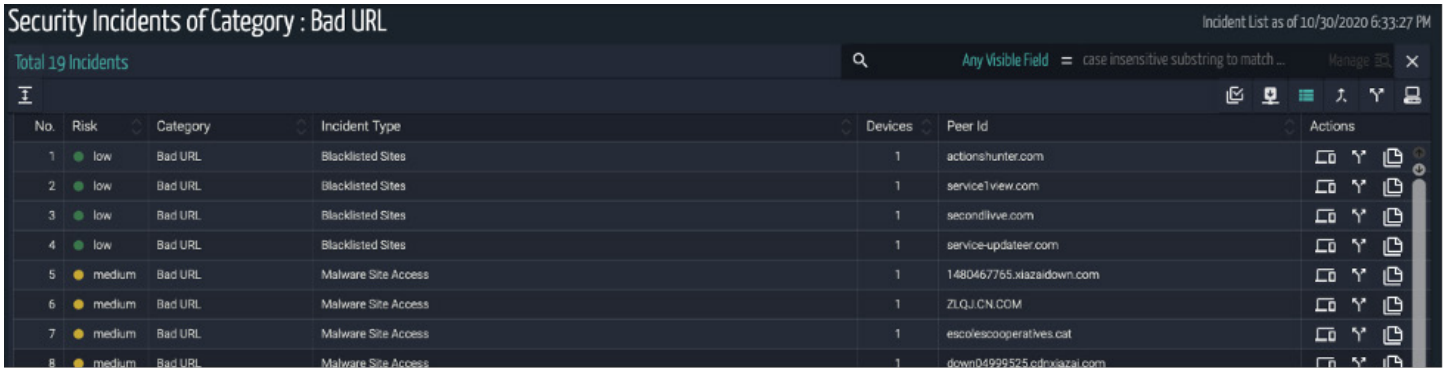
Any organizations security program is only as strong as the weakest link. Every organization is challenged with gaining control over devices that are not under domain control. With Ordr, non-domain managed can be easily identified and make sure they are in compliance.

Active Threat management with Ordr

Threat feed updates:

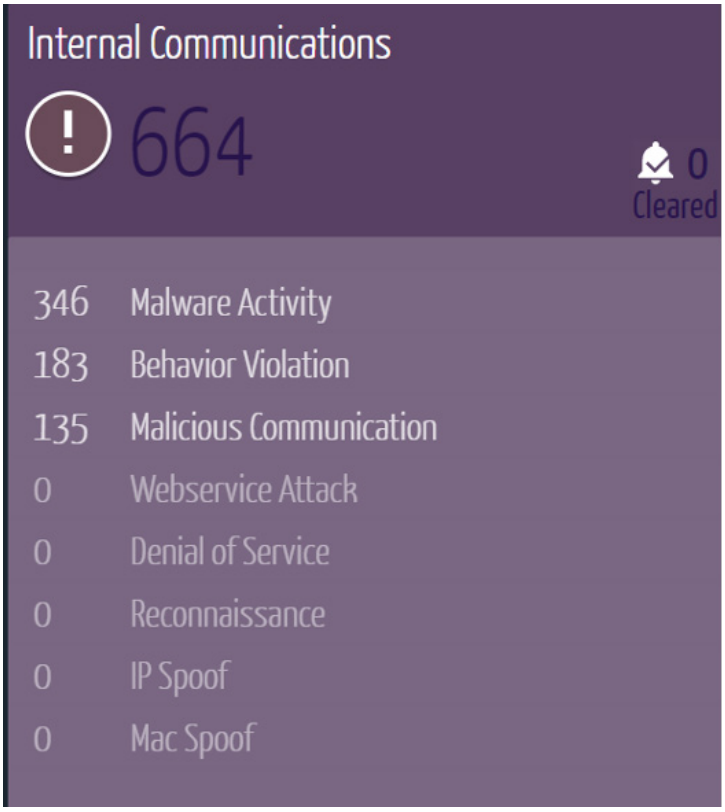
Ordr worked with threat feed providers to update the websites and IP addresses identified by the CISA advisory and other security experts. This service is available for all Ordr customers. Any device initiating communication to these domains and IP addresses will be flagged.





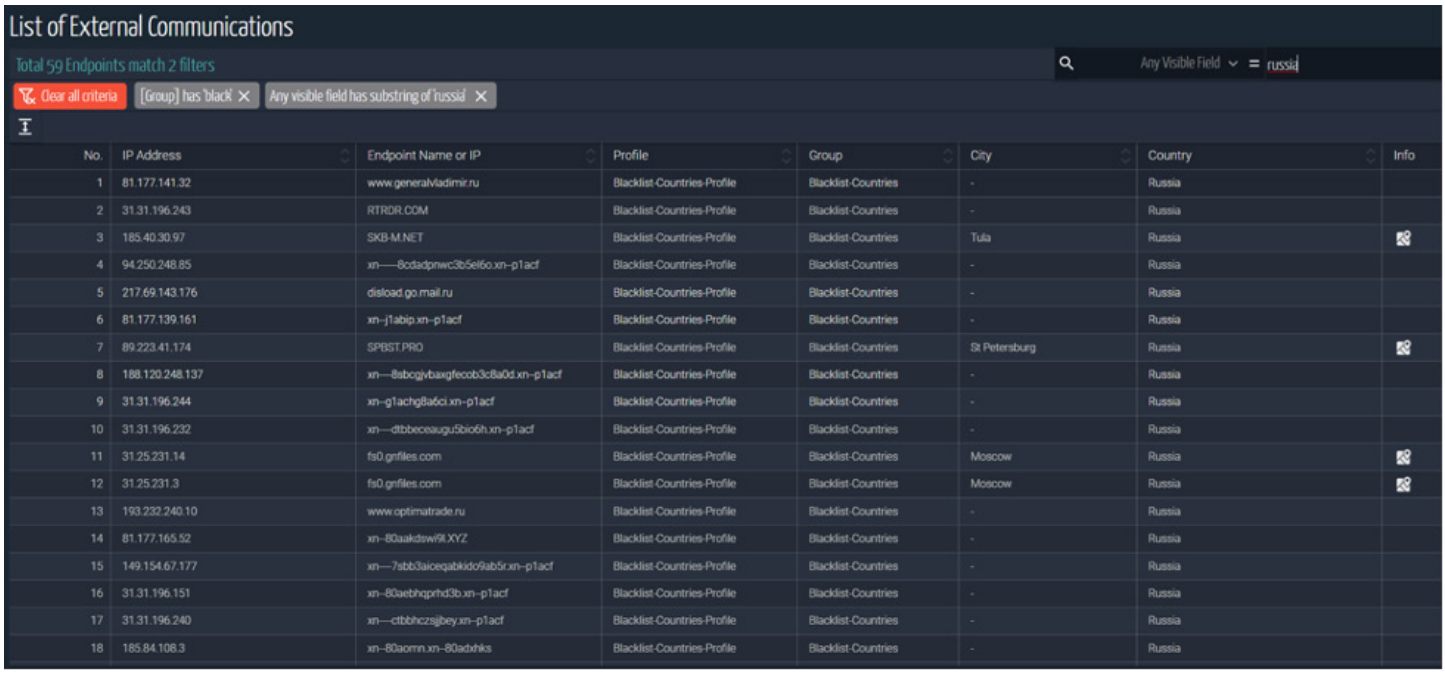
Intrusion detection rules updates:

Ordr has built-in Intrusion Detection engine to monitor active threats. This helps with any East-West propagation of malware which is common in ransomware attacks. The rulesets are up to date to detect and notify any lateral movement of malware.



Monitor external communication:

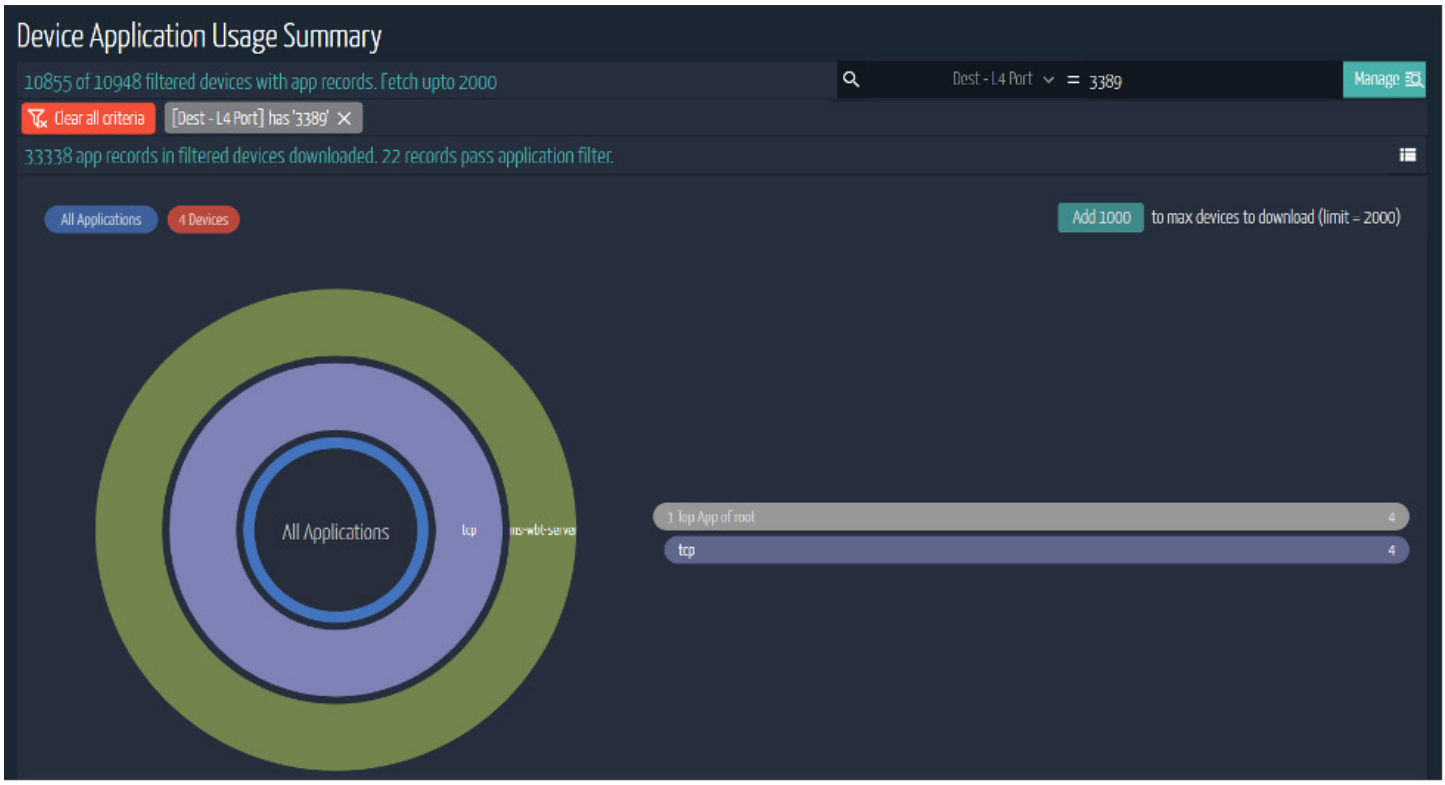
Monitoring external communications is another important step in safeguarding the organization. Ordr provides easy way to monitor device, profile, group communications with easy to use visuals. Note that a communication blocked by a firewall does not mean that the organization is safe. The device that is initiating this communication still need to be identified and fixed.



No.	IP Address	Endpoint Name or IP	Profile	Group	City	Country	Info
1	81.177.141.32	www.generalvladimir.ru	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
2	31.31.196.243	RTRDR.COM	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
3	185.40.30.97	SKB-M.NET	Blacklist-Countries-Profile	Blacklist-Countries	Tula	Russia	
4	94.250.248.85	xn----8cdadpnwc3b5el6o.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
5	217.69.143.176	disload.go.mail.ru	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
6	81.177.139.161	xn--j1abip.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
7	89.223.41.174	SPBST.PRO	Blacklist-Countries-Profile	Blacklist-Countries	St Petersburg	Russia	
8	188.120.248.137	xn----8sbcgjvbaxgfecob3c8a0d.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
9	31.31.196.244	xn--g1achg8a6ci.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
10	31.31.196.232	xn----dtbbeceaugu5bio6h.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
11	31.25.231.14	fs0.gnfiles.com	Blacklist-Countries-Profile	Blacklist-Countries	Moscow	Russia	
12	31.25.231.3	fs0.gnfiles.com	Blacklist-Countries-Profile	Blacklist-Countries	Moscow	Russia	
13	193.232.240.10	www.optimatrade.ru	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
14	81.177.165.52	xn--80aakdswi9l.XYZ	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
15	149.154.67.177	xn----7sbb3aiceqabkido9ab5r.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
16	31.31.196.151	xn--80aebhqprhd3b.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
17	31.31.196.240	xn----ctbbhczsjjbey.xn--p1acf	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	
18	185.84.108.3	xn--80aomn.xn--80adxhks	Blacklist-Countries-Profile	Blacklist-Countries	-	Russia	

Monitor open ports:

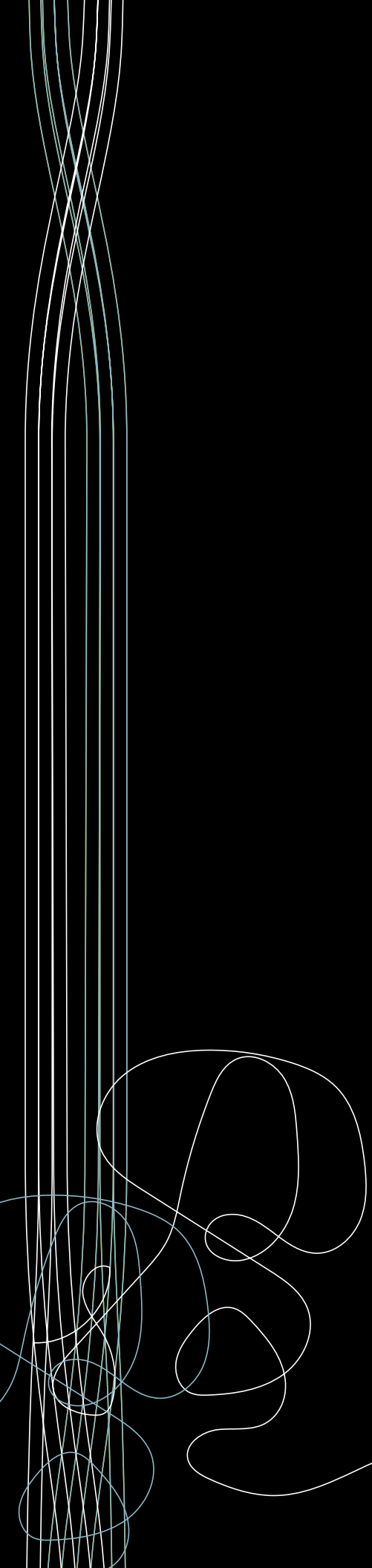
The recent ransomware attacks seem to utilize any open ports to spread the malicious code – specifically port-3389. Ordr monitors all device to device communications and provides an easy way to identify devices that are communicating over port-3389. In lot of cases it is necessary to have to these ports open. Ordr recommends to add this to port to an allow list and let only specified devices to communicate using this port.



For more information on how Ordr can help you identify and manage vulnerabilities for any connected device, please contact **info@ordr.net**.

References:

1. https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/
2. https://cisomag.eccouncil.org/ransomware-attacks-rise-q1-2020/
3. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
4. https://resources.sei.cmu.edu/asset_files/WhitePaper/2020_019_001_644890.pdf
5. https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
6. https://www.justice.gov/criminal-ccips/file/872771/download
7. https://nvd.nist.gov/vuln/detail/CVE-2020-1472



ōrdr

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054