# THE CYBER THREAT AND MUNICIPAL GOVERNMENTS:

## Data from the Field


NETWORK DEFENDER®

The proliferation of cyber attacks against businesses large and small has not spared public organizations like local municipalities and sub-organizations within them (e.g. police and sanitation departments). The ability to easily monetize attacks via untraceable crypto-currencies, combined with largely unfettered access to hacking tools that substantially reduces the expertise necessary to conduct a successful attack, means more opportunistic cyber criminals are moving "down market," eschewing high-risk and high-effort attacks on well-defended household brand name companies for the relatively low-hanging fruit of the small business and small government organization community. In this short paper, we'll provide some data from Network Defender®'s real-world cyber threat detection and blocking platform deployed on the networks of several municipalities to underscore exactly how serious this threat has become to even the smallest communities.

*"...more opportunistic cyber criminals are moving 'down market'... for the relatively lowhanging fruit of the small business and small government organization community."*

## BACKGROUND

Network Defender is delivering an advanced cyber security technology that identifies likely malicious devices (via their IP addresses) connecting to the networks of local municipalities, school districts, and other local government entities. The service has been deployed to date on over 1,000 networks, affording Network Defender the ability to collect data anonymously from local organizations in the wild, facilitating analyses like this one. Below, we present actual traffic data from 16 local government entities, illustrating the kinds of threats typically encountered by these networks in today's threat environment on a daily basis.

*"Network Defender is delivering an advanced cyber security technology that identifies likely malicious devices...connecting to the networks of local municipalities, school districts, and other local government entities."*

The Network Defender platform calculates a cyber risk score for every IP attempting to connect to the local government network, and then autoblocks the highest risk connections, or the ones with the highest probability of being the source of nefarious activity. The calculated score varies on a scale from 1 to 9, where 9 indicates the highest risk connection, and very likely a threat to the network.

*"The Network Defender platform calculates a cyber risk score for every IP attempting to connect to the local government network, and then autoblocks the highest risk connections."*

As the table below indicates, some local entities saw only a handful of threats in the 30-day period over which the data was collected, while others experienced hundreds of connections from high risk devices over the public internet. For the data listed in the table below, the average number of level-9 threats in this 30-day period was 168, while the median was 129, meaning, the average municipality, or municipal departments, is exposed to about 4 high-risk threat connections per day.

It's important to note, that with few exceptions, none of these 9-level threats - none of which have any legitimate reason to connect to a local government network - was blocked by the firewall of the municipality, despite the reality that many of those small businesses subscribed to the firewall manufacturers' native threat intelligence feed. The Network Defender solution is therefore identifying and blocking threats beyond those caught by the firewall, underscoring the benefit of a "layered" security "stack," a universal best practice across the cyber security community.

*"... the average number of {highest risk threats} in this 30-day period was 168, while the median was 129, meaning, the average municipality, or municipal departments, is exposed to about 4 highrisk threat connections per day."*

1 https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/

| LOCAL GOVERNMENT ENTITY | TOTAL NUMBER OF 9-LEVEL THREATS IN MAY 2022 | TOTAL NUMBER OF CONNECTION ATTEMPTS BY 9-LEVEL THREATS | TOTAL NUMBER OF 8-LEVEL THREATS IN MAY 2022 | TOTAL NUMBER OF CONNECTION ATTEMPTS BY 8-LEVEL THREATS |
|---|---|---|---|---|
| Northern US Town Offices - Population 2,200 | 1 | 2 | 1 | 20 |
| Northwest US Town Offices - Population 3,600 | 2 | 5 | 2 | 5 |
| Northern US Town Offices - Population 18,000 | 410 | 2,978 | 229 | 925 |
| Northeast US Town Offices - Population 14,000 | 69 | 91 | 23 | 46 |
| Northeast US Town Offices - Population 7,600 | 404 | 1,344 | 224 | 1,408 |
| Northeast US Town Offices - Population 17,000 | 429 | 1,431 | 960 | 2,030 |
| Northern US Town Offices - Population 3,000 | 22 | 22 | 1 | 2 |
| Northern US Town Offices - Population 22,300 | 324 | 873 | 169 | 927 |

| LOCAL GOVERNMENT ENTITY | TOTAL NUMBER OF 9-LEVEL THREATS IN MAY 2022 | TOTAL NUMBER OF CONNECTION ATTEMPTS BY 9-LEVEL THREATS | TOTAL NUMBER OF 8-LEVEL THREATS IN MAY 2022 | TOTAL NUMBER OF CONNECTION ATTEMPTS BY 8-LEVEL THREATS |
|---|---|---|---|---|
| Southern US Town Offices - Population 4,300 | 190 | 947 | 104 | 374 |
| Southern US K-12 School District | 235 | 955 | 149 | 448 |
| Western US K-12 School District | 246 | 330 | 177 | 217 |
| Western US Local Housing Authority | 207 | 711 | 142 | 640 |
| Waste Water Division of Northeast Town | 41 | 52 | 5 | 11 |
| Northeast Town Department of Public Works | 46 | 62 | 22 | 39 |
| Northeast Town Library | 63 | 70 | 19 | 37 |
| Northeast Town Police Department | 8 | 12 | 4 | 132 |

[5] https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

## IS A "9" REALLY THAT DANGEROUS?

If the Network Defender threat detection and blocking platform is scoring an IP a 9, you can feel comfortable concluding that that 9-level device has no business connecting to the network of the small business. It is, however, reasonable to ask "why not"? To answer that question, we've provided some examples below of 9-level threats detected on the networks of our MSP partners' clients recently.

- An Iranian Telecom company identified for exploiting SQL server vulnerabilities attacking a K-12 school district in the Southeast US
- A Chinese device associated with brute force attacks (automated attempts to identify weak passwords) also attacking the K-12 school district's offices
- A German IP launching a Telnet open port scan and potential SNMP (Simple Network Management Protocol) attack was stopped attempting to connect to an animal hospital in the US
- A Chinese host scanning for, and then potentially attacking, a web application vulnerability in the ThinkPHP, attacking the offices of a specialty pharmacy chain
- A known phishing site in Germany connecting to the network of a State Regulatory Agency office in the southern US
- A host - located in the US - associated with brute force SSH attacks (the objective of which is to use the SSH protocol to execute commands on a remote computer) was blocked by Network Defender on the network of the offices of a small municipality in the southwest US
- Servers running Shodan scanning software that catalogs internet-facing devices and software. Shodan data is used primarily by pen testers and hackers to more efficiently identify their targets.
- Command and control servers for the Mirai botnet, malware that hijacks target devices and uses them in DDoS attacks
- A command and control server for Redline Stealer malware, which harvests sensitive information from infected machines

***"....none of these 9-level threats - none of which have any legitimate reason to connect to a local government network - was blocked by the firewall of the municipality."***

A firewall is an essential element of a security architecture for all size organizations, and has been for decades. But, because the threat landscape evolves literally by the hour, firewalls require care and feeding to be effective. Very few organizations, especially local municipalities, have the resources to manage the most critical element of the firewall - the blocklist - actively and continuously. As is clear from the data we've assembled and presented here, that's exactly where Network Defender's automated solution comes in.

## ABOUT CELERIUM

Celerium® powers active cyber defense solutions to help protect organizations and communities from increasing cyberattacks. With a rich 16-year history of facilitating cyber threat sharing for critical industry sectors and government agencies, Celerium is an established leader in providing innovative cybersecurity solutions, with solution directions based on the evolving needs of the industry.

Learn more at **www.Celerium.com** and follow us on X at **@CeleriumDefense**

CELERIUM.com