Transforming Network Data into Cyber Intelligence for State and Local Agencies

Without a doubt, the volume and frequency of cyberattacks have increased in the wake of the COVID-19 pandemic. Cybercriminals are taking advantage of the increase in endpoints and security lapses due to remote work to step up the number of attacks.

Attacks on state and local governments are rising in frequency. In 2019 alone, there were 140 ransomware attacks—an average of 3 per day—targeting public, state and local government and healthcare providers. This is up 65% from the previous year.[1]

Yet state and local agency cybersecurity efforts have not kept up. While 60 percent of government agency respondents describe the maturity level of their organization's cybersecurity program as mature, only 38 percent of state and local respondents say their agencies have achieved that level of maturity in their cybersecurity initiatives.[2]

The stakes are high. According to IBM's Cost of a Data Breach 2020, the average cost of a breech is $3.86 million. The average time to identify and contain a breach is 280 days; 207 days to identify a breach and 73 day to contain it.

Given the lack of detection and prevention, it's not surprising that 90% of security experts are not satisfied with the speed and capabilities they have in detecting incidents.[3] Clearly, a different approach is required—one that detects threats already in the network.

Network Detection and Response

Network Detection and Response (NDR) solutions transform network visibility into security intelligence, providing essential analytics and forensics for broad threat detection, investigation and mitigation. By capturing and storing all network packet and flow data in real- or near real-time across your agency (both north/south as well as east-west traffic) and leveraging analytics to identify suspicious traffic, it delivers the crucial insights to detect and investigate advanced threats that bypass typical preventative measures, as well as those that originate inside the network.

Unprecedented Visibility

Riverbed® NetProfiler Advanced Security Module is Riverbed's NDR. It is an add-on module to Riverbed NetProfiler, leading network traffic monitoring. They both leverage NetProfiler's ability to capture and store all flow data all the time so the data you need is always available for analysis.

[1] https://securityboulevard.com/2020/01/cyber-attacks-against-state-and-local-governments-surge/

[2] https://fcw.com/pages/hpsp/hpsp-10.aspx

[3] RSA, Threat Detection Effectiveness Survey 2016

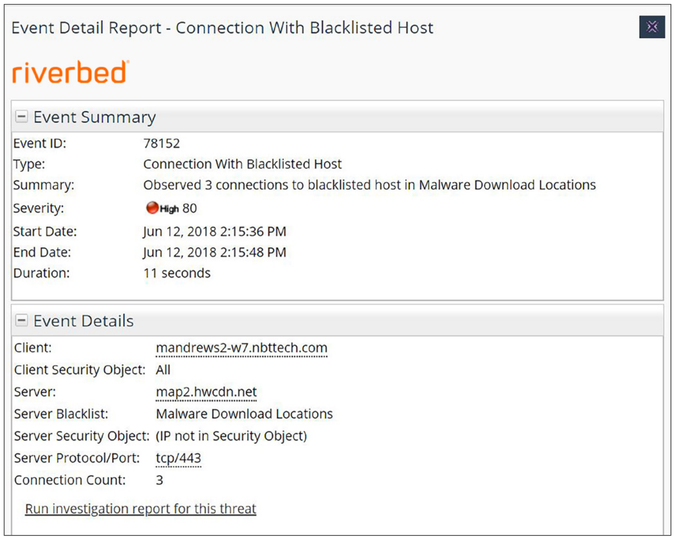
NetProfiler Advanced Security Module offers a wide range of detection capabilities, including:

- **Security analytics**: examines network traffic and compared it to historical baseline to identify threats that generate unusual traffic patterns, such as zero-day events, unexpected new services, hosts, or connections
- **Data exfiltration**: detects when large volumes of data are staged or move out of your network unexpectedly
- **DDoS detection**: quickly identifies a wide range of DDoS attacks and automatically triggers mitigations or black hole routes
- **Blacklisted communications**: alerts you when your system communicates with known malware, viruses, spyware, etc., so you can investigate and take action
- **Incident forensics**: provides full historical details so you get the complete scope of the attack; drill into the packets for even more details
- **Threat hunting**: Leverage full forensic records to investigate post-compromise

Threat Intelligence for Situational Awareness

Threat intelligence is evidence-based information that identifies emerging threats and helps you mitigate your agency's exposure to them. NetProfiler Advanced Security Module shows you where threats may exist in your environment so you can swiftly act on them. It provides two types of threat intelligence, which are updated regularly:

- **Blacklists** detail known malicious or suspicious entities that should not be allowed access to your network. The NetProfiler Advanced Security Module correlates blacklisted items to your environment and alerts on positive matches so you can stop the communication. Event detail is available for further research on the threat. At any time, you can add new threats to your blacklist as you run across them in your security landscape.



Event Detail Report - Connection With Blacklisted Host

riverbed

Event Summary

Event ID: 78152
Type: Connection With Blacklisted Host
Summary: Observed 3 connections to blacklisted host in Malware Download Locations
Severity: High 80
Start Date: Jun 12, 2018 2:15:36 PM
End Date: Jun 12, 2018 2:15:48 PM
Duration: 11 seconds

Event Details

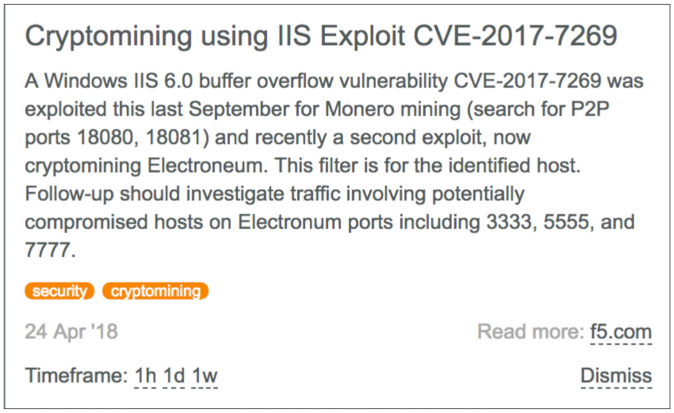
Client: mandrews2-w7.nbttech.com
Client Security Object: All
Server: map2.hwcdn.net
Server Blacklist: Malware Download Locations
Server Security Object: (IP not in Security Object)
Server Protocol/Port: tcp/443
Connection Count: 3

Run investigation report for this threat

Figure 1

An example of an event detail report showing a connection to a blacklisted host with supporting info and links to investigative reports for the threat..

- **Threat feeds** are analyst-generated information about potential threats that may or may not mean your network has been compromised. Threat feeds can include topics like Shodan activity and cryptocurrency mining that could be legitimate traffic, but might also hide malicious activity. The alert provides you with resources to learn more and the links to investigate the potential vulnerability in your environment.



Cryptomining using IIS Exploit CVE-2017-7269

A Windows IIS 6.0 buffer overflow vulnerability CVE-2017-7269 was exploited this last September for Monero mining (search for P2P ports 18080, 18081) and recently a second exploit, now cryptomining Electroneum. This filter is for the identified host. Follow-up should investigate traffic involving potentially compromised hosts on Electronum ports including 3333, 5555, and 7777.

security cryptomining

24 Apr '18

Read more: f5.com

Timeframe: 1h 1d 1w

Dismiss

Figure 2

An example of a threat feed. You can read more about it, or explore your environment for signs Electronum on ports 3333, 5555, or 7777 in the past 1 hour, 1 day, or 1 week.

DDoS Detection and Mitigation

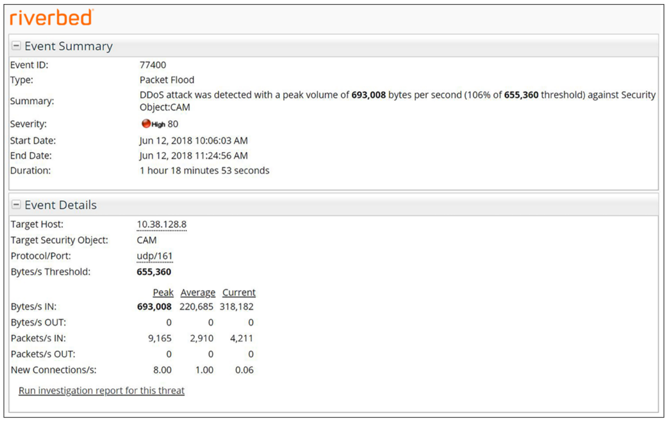
DDoS detection no longer needs to be a dedicated solution, so you need fewer vendors in the NOC/SOC. NetProfiler Advanced Security Module accurately identifies all types of DDoS attacks fast—in just 10 to 30 seconds—and acts immediately and surgically. Redirect traffic to an A10 TPS DDoS scrubber or other mitigations so DDoS traffic is dropped while the rest of your network continues to operate normally.

Security Analytics

Worried that threats are slipping through the cracks? NetProfiler Advanced Security Module learns and understands the changing patterns of behavior in your network to combat both insider and external threats. It provides dynamic visibility into the applications and traffic flowing throughout your network.

Out of the box, the security analytics classifies threats into these broad categories:

- **Suspicious connection**: when two hosts that do not normally communicate with one another start communicating (for example, those state and local agencies that act as MSP for other smaller agencies, there can be many new connections that are suspicious, and should be check out. This is an easy way for bad guys to get in unnoticed.)
- **Worm**: a pattern of scanning among hosts, where systems previously scanned suddenly become scanners themselves. Identification of patient zero, infected hosts and means of propagation are reported
- **New host**: a host that has not been previously identified has sent enough traffic to be regarded as having joined the network
- **New service**: a host or an automatic host group is providing or using a service over a new port
- **Host scan**: a series of hosts on the monitored network being interrogated on the same port
- **Port scan**: a host or series of hosts on the monitored network being interrogated across a range of ports
- **Bandwidth surge**: a significant increase in traffic that conforms to the characteristics of a Denial of Service (DoS) or a Distributed Denial of Service (DDoS) attack



riverbed

⊟ Event Summary

Event ID: 77400
Type: Packet Flood
Summary: DDoS attack was detected with a peak volume of **693,008** bytes per second (106% of **655,360** threshold) against Security Object:CAM
Severity: ● High 80
Start Date: Jun 12, 2018 10:06:03 AM
End Date: Jun 12, 2018 11:24:56 AM
Duration: 1 hour 18 minutes 53 seconds

⊟ Event Details

Target Host: 10.38.128.8
Target Security Object: CAM
Protocol/Port: udp/161
Bytes/s Threshold: **655,360**

	Peak	Average	Current
Bytes/s IN:	**693,008**	220,685	318,182
Bytes/s OUT:	0	0	0
Packets/s IN:	9,165	2,910	4,211
Packets/s OUT:	0	0	0
New Connections/s:	8.00	1.00	0.06

Run investigation report for this threat

Figure 3

An example of a DDoS alert.

Threat Hunting

Cyber threat hunting starts with the premise that bad actors have already breached your perimeter defenses and are operating inside your network. An analyst starts with a hypothesis about how an attacker might have breached your defenses, and then proactively and iteratively tries to find the evidence to support the hypothesis—the systems compromised, and the data accessed, etc. Along the way, the results of the investigation typically cause the analyst to pivot in other more fruitful directions.

Full fidelity flow and packet data are critical for detecting and disrupting active attack activities. It provides both the breadth and depth of visibility you need to gain insight across the entire agency—the insight needed for cyber threat hunting. One-click access to packet data also supplements your flow data.

In addition, the Advanced Security Module provides rich security analytics and threat hunting workflows that improve your ability to uncover hidden and entrenched threats. They let you search the network for evidence and footholds and then pivot on promising leads that ultimately determine how the intruder is controlling compromised assets.

Professional Services

Your purchase of the NetProfiler Advanced Security Module includes configuration and deployment professional services that Riverbed Professional Services (RPS) will deliver. These services are designed to ensure that the initial configuration of the NetProfiler Advanced Security Module is based on Riverbed's best practices and deliver the security insights and business value described in this brochure. They will include a review of your network architecture, desired security policy, and requirements. RPS will perform the applicable data analysis and configuration of your NetProfiler Advanced Security Module remotely in conjunction with your designated subject matter experts and help ensure you get maximum value out of your NetProfiler Advanced Security Module purchase through expert configuration based on best practice compliance.

Value Delivered

The NetProfiler Advanced Security Module provides full visibility into the activities of threat actors with real-time and forensic capabilities to ensure even the most evasive attackers have no place to hide. As a result, you can reduce your risks, lower your financial exposure, and protect your citizen data.

To learn more about Riverbed NetProfiler Advanced Security Module, click here.

About Riverbed
Riverbed enables organizations to maximize performance and visibility for networks and applications, so they can overcome complexity and fully capitalize on their digital and cloud investments. The Riverbed Network and Application Performance Platform enables organizations to visualize, optimize, remediate and accelerate the performance of any network for any application. The platform addresses performance and visibility holistically with best-in-class WAN optimization, network performance management (NPM), application acceleration (including Office 365, SaaS, client and cloud acceleration), and enterprise-grade SD-WAN. Riverbed's 30,000+ customers include 99% of the *Fortune* 100. Learn more at riverbed.com.

riverbed®