LOOKINGGLASS

CASE STUDIES

Supporting Threat Hunting Missions

We develop cybersecurity solutions that empower organizations to meet their missions with tailored, actionable threat intelligence. In this white paper, we highlight specific threat intelligence and analysis from recent 2021 cyber attacks.

EXECUTIVE SUMMARY

In today's fast-moving cybersecurity environment, cyber threats are evolving at an unprecedented rate, making it challenging to proactively track emerging threats to your networks, third-party vendors, and your supply chain ecosystem. Compounding this is the massive and complicated collection process that is required to sift through huge volumes of raw data to pinpoint intelligence that is timely, relevant, and actionable to your organization, based on your risk tolerance and cybersecurity posture.

LookingGlass Cyber Solutions™ addresses these cybersecurity challenges head on, empowering organizations to meet their missions with tailored, actionable threat intelligence and active defense capabilities delivered at machine speed.

LookingGlass today serves the most sophisticated government organizations, Fortune 500 companies, and critical telecommunications firms, enabling them to see what an adversary can see of their infrastructure from the public internet and providing them with best-in-class network security, continuous assessments of the attack service (whether cloud or hybrid), and threat mitigation tools.

As companies rely on an ever-widening ecosystem of suppliers and third party providers, cyber risks and attacks are multiplying. While being more interconnected creates efficiencies and strengthens business operations, it also increases one's attack surface, potential attack vectors, and overall cyber risk.

This document features actionable threat intelligence and analysis produced by LookingGlass, highlighting the support LookingGlass provides for clients around the country. It also highlights testimonials from Threat Hunters, State Fusion Center teams and Cyber Analysts at federal, state and local governments, underscoring the value LookingGlass brings to its clients.

© 2021 LookingGlass Cyber Solutions, Inc. All rights reserved.

USE CASE: OPTIMIZING THREAT HUNT AND SUPPORTING INCIDENT RESPONSE

Pulse Secure Vulnerabilities

The Situation:
April 20, 2021: DHS releases Emergency Directive 21-03 about Pulse Connect Secure Product Vulnerabilities

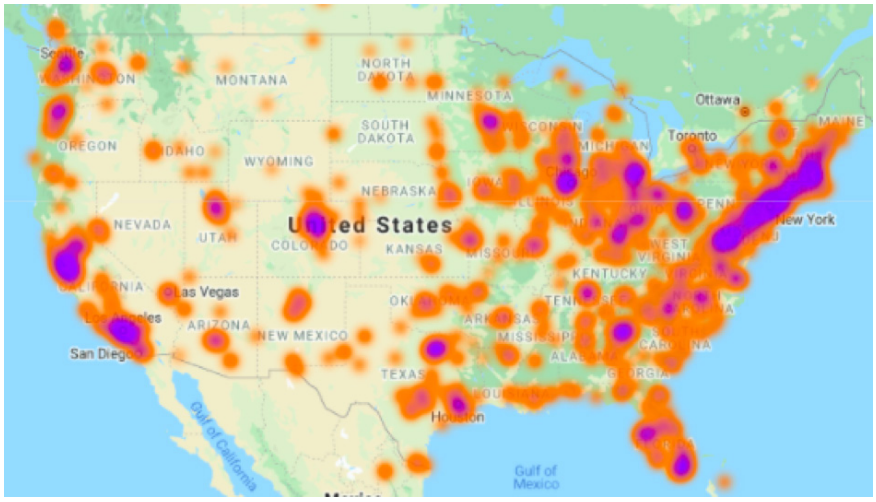
Our Approach:
- Immediately configured the LookingGlass Suite to discover which internet-connected assets had the Pulse Secure vulnerabilities
- Automatically enriched findings with additional threat intelligence to discover other risk and exposures
- Mapped potentially vulnerable assets geographically and conducted sector analysis to determine sector risk

Findings and Outcomes:
- The LookingGlass Suite found approximately 18,500 network assets within the continential U.S. (CONUS) that were potentially exploitable/vulnerable with the Pulse Secure attack vectors
- Provided customers with detailed information regarding assets within their domain/IP range that were vulnerable, including identifying additional attack vectors
- Internet footprinting provided customers with geographic location of assets to better assist on-the-ground coordination across enterprise operations.

CISA EMERGENCY DIRECTIVE

"CISA has determined that this exploitation of Pulse Connect Secure products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action.

This determination is based on the current exploitation of these vulnerabilities by threat actors in external network environments, the likelihood of the vulnerabilities being exploited, the prevalence of the affected software in the federal enterprise, the high potential for a compromise of agency information systems, and the potential impact of a successful compromise."



May 11, 2021: Country-level view of vulnerable Pulse Secure assets in CONUS

"LookingGlass is one of the few tools I have where I can go in and easily research for a specific hash, IP address, or actor group that is related an alert. On that front, it is one of my first go-to solutions.

If we lost LookingGlass, it would take us a lot more time to hunt and get the results we're looking for in a search."

– Threat hunter, U.S Federal Department

USE CASE: OPTIMIZING THREAT HUNT AND SUPPORTING INCIDENT RESPONSE

(Continued...)

Pulse Secure Vulnerabilities

May 11, 2021: Approximately 12,500 internet-connected assets still exhibiting the Pulse Secure vulnerabilities within CONUS (see map on previous page)

Critical Infrastructure Sector	Number of Organizations
Chemical	9
Commercial Facilities	62
Critical Manufacturing	13
DIB	19
EDU	147
Energy	43
Food & Agri	23
FinServ	94
Healthcare	92
Transportation Sys	28
Water/Wastewater	3
Government – Civilian	35
Government – Defense	4
Government – State, Local, & Tribal	159

Note: count in the communications/IT sector was too large to properly categorize in a timely manner.

© 2021 LookingGlass Cyber Solutions, Inc. All rights reserved.

USE CASE: DETERMINING CYBER RISK & EXPOSURES WITH DIGITAL, INTERNET FOOTPRINTING

FL Water Treatment Plant Attack

The Situation:
February 8, 2021: Pinellas County Sheriff's Office holds news conference detailing an attack on the Bruce T. Haddock (BTH) Water Treatment Plant in Oldsmar, FL.

The attack was noted by a plant operator on February 5, 2021, who witnessed abnormal behavior during the course of normal operations. However, the operator dismissed it because supervisors can remotely access systems for monitoring purposes.

Hours later, the operator noticed that multiple programs were open and chemical levels in the water had changed to dangerous levels.

The Bruce T. Haddock (BTH) Water Treatment Plant does not own any public-facing internet infrastructure, instead leveraging the City of Oldsmar's systems.

Our Approach:

- Reviewed publicly available information about the attack
- Queried our vast database of deep, dark web intelligence for chatter about water treatment plants or water districts
- Configured the LookingGlass Suite to gather information about
- internet-connected assets tied to the victim (i.e., City of Oldsmar)
- Based on enriched threat intelligence that highlighted other risk and exposures, conducted open source intelligence gathering, specifically around potentially vulnerable open port (Port 4443)

"...the onboarding process [for LookingGlass was] the easiest I've ever had for a tool... we are able to consolidate a variety of threat intelligence into one platform. This allows for both ease of use and being able to evaluate threats more consistently.

Also, it's a trusted platform – LookingGlass keeps information on my indicators totally confidential. I don't have to worry that what I load into scoutPRIME is going to end up on the internet. That trust is huge for us."

– State Fusion Center Cyber Lead

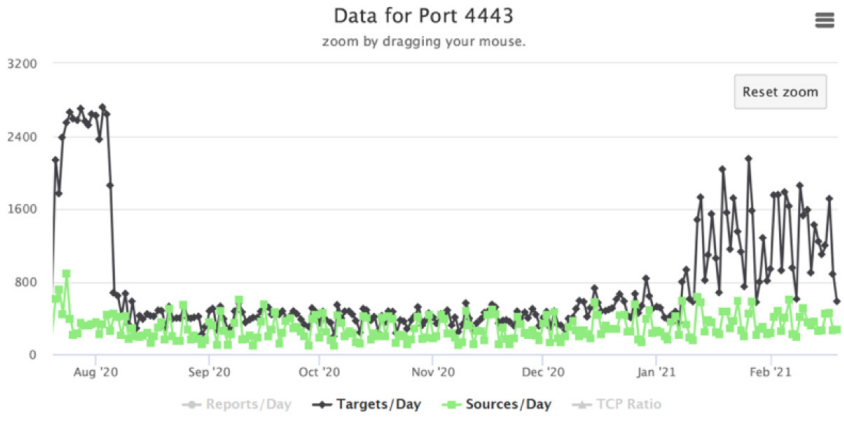


Image & data from https://isc.sans.edu/port.html?port=4443. Accessed: 2/19/2021

"[LookingGlass] identified a C2 network tied to a massive ransomware infection that impacted networks. A search warrant was issued based off the scoutPRIME data and the infected host was seized.

The investigation determined who the host belonged to and how the infection entered the network. Without scoutPRIME, we would not have found the patient zero host before damaged occurred."

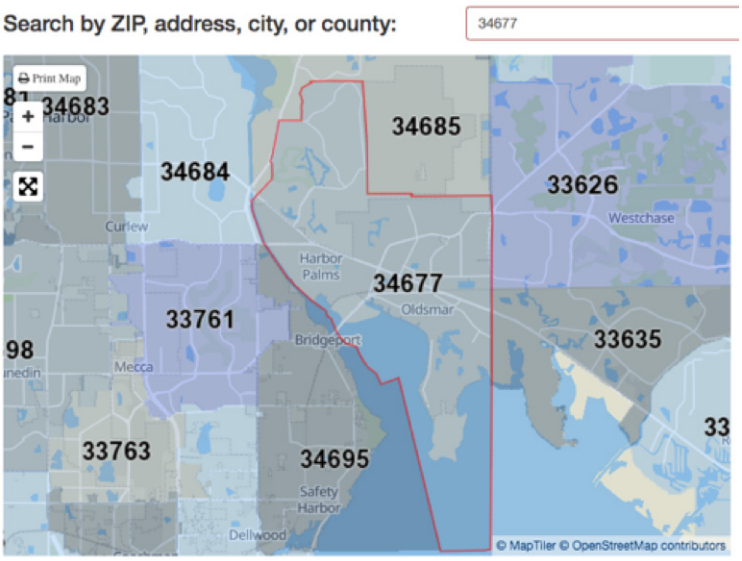
– State Fusion Center Cyber Lead

USE CASE: DETERMINING CYBER RISK & EXPOSURES WITH DIGITAL, INTERNET FOOTPRINTING

(Continued...)

Findings/Outcomes:

- Discovered a potential breach/compromise of a US-based water district with a population around 20,000 in 2020.
- Found multiple Compromised Account Credentials (CACs):
  - 24 CACs for myoldsmar[.]com; 6 discovered in 2020
  - 2 users have "password" as their password
  - 44 CACs for ci[.]oldsmar[.]fl[.]us; 2 discovered in 2020
- Significant attack activity for Port 4443 based on SANS Internet Storm Center data
  - Aug 3, 2020: 2719 targets
  - Aug 8, 2020: 425 targets
  - Jan 26, 2021: 2152 targets
  - Feb 5, 2021: 1785 targets - Date of the attack
  - Feb 8, 2021: 609 targets - Date of Pinellas County Sheriff's news conference



34677: Oldsmar, FL and Harbor Palms, FL, with a combined population of 20,842

© 2021 LookingGlass Cyber Solutions, Inc. All rights reserved.

ABOUT LOOKINGGLASS

LookingGlass develops cybersecurity solutions that empower organizations to meet their missions with tailored, actionable threat intelligence and threat mitigation capabilities that move at machine speed. For more than a decade, the most advanced organizations in the world have trusted LookingGlass to help them protect financial systems, ensure telecommunications are cyber-resilient, and safeguard national security interests.

Finding a needle in the haystack.

We help our clients continuously monitor their own and their third-party vendor's networks to keep your organization safe. Our LookingGlass platform is purposefully designed to provide just this mix of features so you can assess and manage supply chain and third-party risk information at scale.

Our unique footprinting capability gives your security staff an "adversary's view" of your third parties, so you can truly understand any vulnerable supply chain network dependencies, allowing you to get ahead of third-party risks and breaches.

Our customizable threat actor modeling enables your security analysts to track adversary capabilities and motivations, so you can understand how your organization, sector, or ecosystem could be attacked and implement security controls before that happens.

Contact us at info@lookingglasscyber.com to learn more about our work.

"We help organizations identify how a hacker got in, what vulnerability they exploited, and what mitigation needs to be put into place. But we also have to determine the real-life identity of that hacker and then prove beyond a reasonable doubt in a court of law that this person committed this crime…

LookingGlass provides the data, in whatever format we need, that helps pinpoint and prioritize what and where we need to be looking to jumpstart our investigations. Without LookingGlass, some of our most effective operations would slow to a crawl or stop."

– Lead Cyber Analyst
Federal Agency


LOOKINGGLASS