DS/{LABS}

A GLOBAL RESET

Cyber Security 2021

2020 AN UNPRECEDENTED YEAR IN CYBER-ATTACKS

The most reliable way to **predict** the future is to **create it**.

—Abraham Lincoln

The reach of Cyber-Attacks is expanding. Millions of new applications, growing cloud adoption and the increase in connected devices are creating challenges that security teams need to properly protect and manage. Organizations are feeling the pressure to keep pace with the threat volume resulting from so many potential entry points.

Cyber-Criminals are continuing to be more sophisticated. While traditional cyber threats continue, sophistication of advanced attacks are increasing. As a result, organizations are challenged to keep pace with threat evolution.

Security teams are constrained due to the Cyber Skills shortage. The cybersecurity industry faces a skills gap that has become a top emerging risk for organizations. There are not enough skilled professionals available to properly triage, investigate and respond to the growing number of threats, making it easier for cybercriminals to outpace legacy security processes and tools.

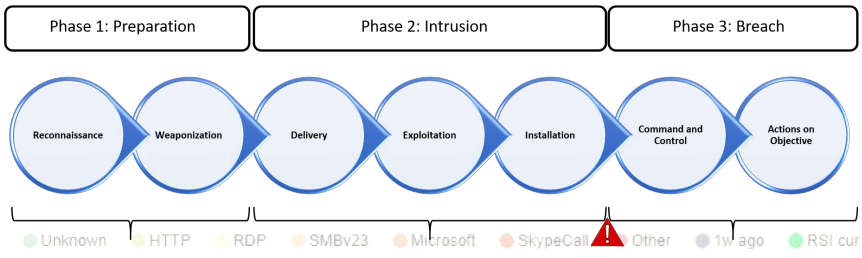
We are in a period of economic uncertainty, and **validation** will help **ensure** organizations are maximizing their **return on their cyber security investment**.

SUPPLY CHAIN EXPLOIT (SCE): AN ADVANCED CYBER-ATTACK DEFINED

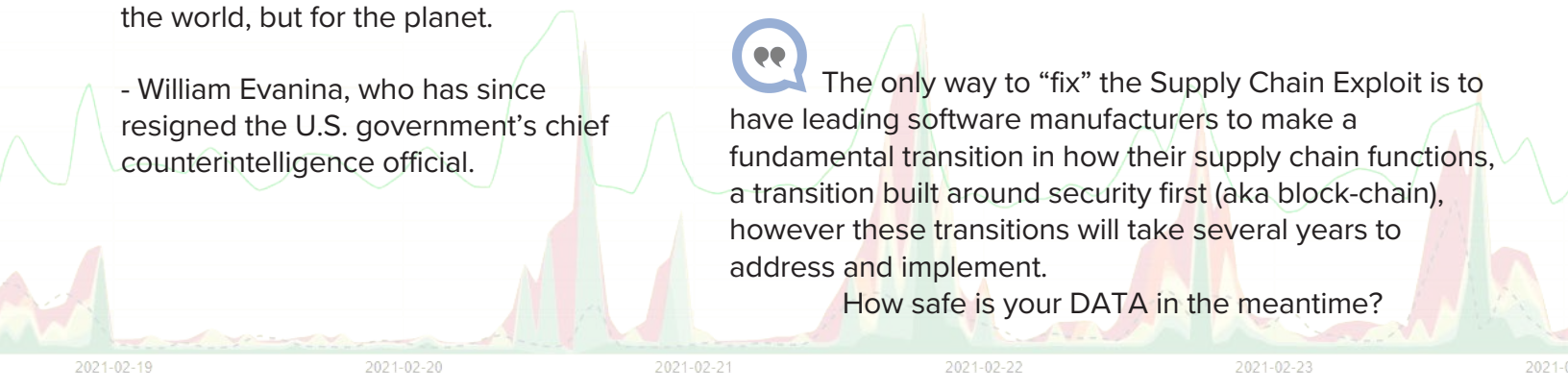
A supply chain exploit is when hackers gain access to organizations by slipping their malware into software updates. The attack relies on a trusted relationship between the targeted organization and the software provider. When users update their systems they unwittingly invite a Trojan horse into their computer networks. The bigger issue is that it can take months before the exploit is discovered. Then there is often a complicated investigation that has to take place to discover the extent of the information effected.

> We're going to have to wrap our arms around the supply-chain threat and find the solution, not only for us here in America as the leading economy in the world, but for the planet.
>
> - William Evanina, who has since resigned the U.S. government's chief counterintelligence official.

The Cyber Kill Chain



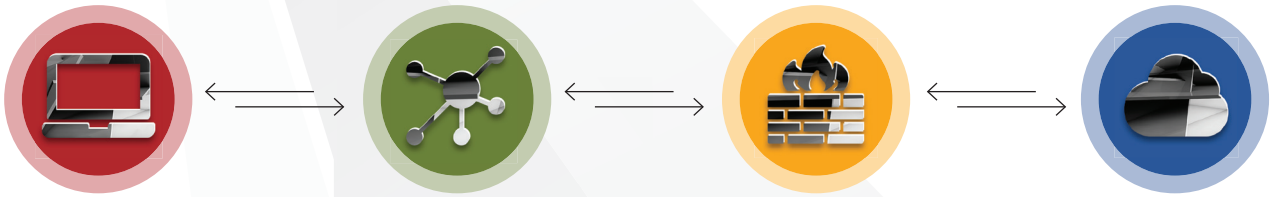
> The only way to "fix" the Supply Chain Exploit is to have leading software manufacturers to make a fundamental transition in how their supply chain functions, a transition built around security first (aka block-chain), however these transitions will take several years to address and implement.
>
> How safe is your DATA in the meantime?



n@d@r provides layer 7 (application) data, to know who's talking to whom.

Despite the urgency of their work, threat actors will continue to **target healthcare** providers and **private enterprise.**

CYBER **SECURITY** **TAKING** THE **LIMELIGHT**



It's time for a change in network security!

At this point in time NO cyber security software or appliance can stop the exploitation of supply chain vulnerabilities, regardless of their claims. It is a simple fact. The only option organizations have is to STOP the data from leaving their networks, is to identify the offending software/ computer and take action to remove the threat actor. But how exactly do you go about doing just that?

Introducing n@d@r

n@d@r or "Network Anomaly Detection And Response", is an AI/ML driven cyber security device designed to trap cyber-attacks within the local network preventing them from transmitting your confidential data to the threat actor.

Through the utilization of globally standardized architectures, proven OSI framework and ack/ syn behavior analysis, n@d@r provides your network with an autonomous gatekeeper.

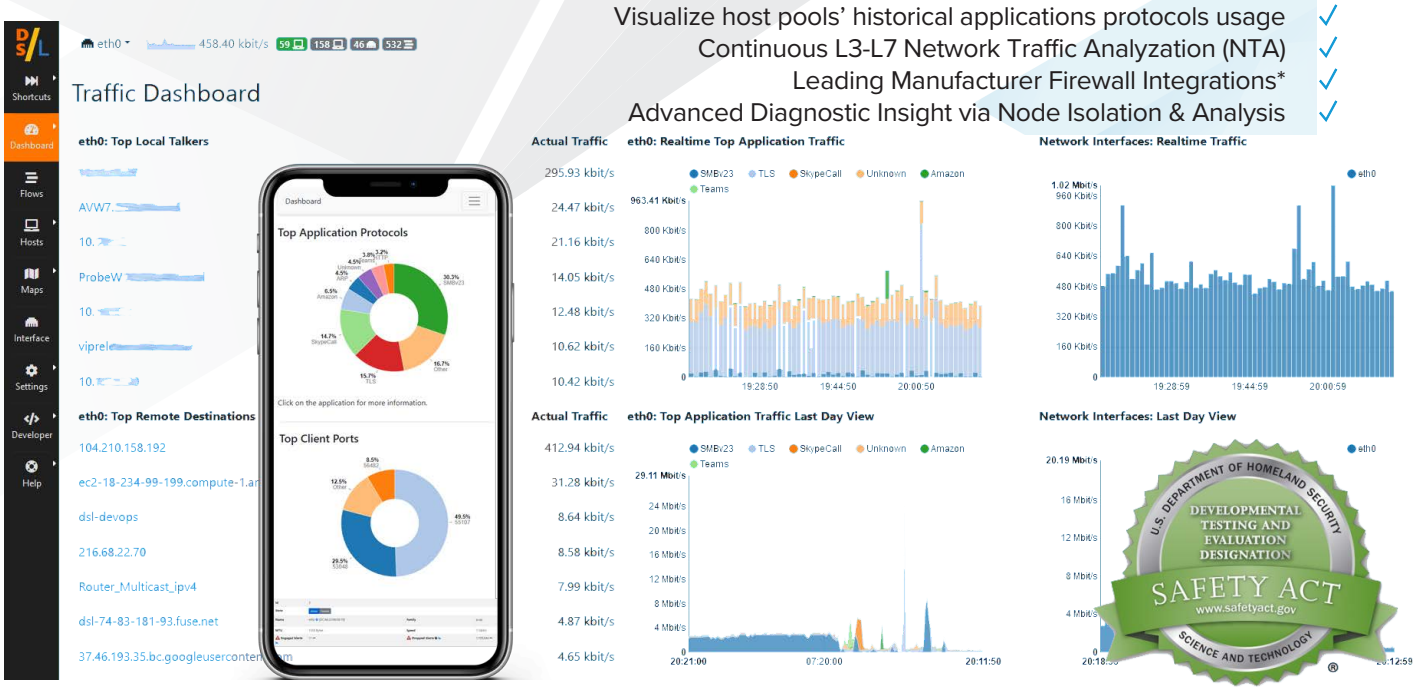
Users and Corporations alike will no longer be at the mercy of software providers and their production exploits. In the event a supply chain exploit is utilized against a software manufacturer, if you have deployed n@d@r, you can be confident in the fact that your confidential information is safe.

Integrating with industry leading firewall manufacturers and XDR technologies, n@d@r can autonomously shut down fraudulent traffic with little to no interaction from IT personnel. Rendering any exploit null, BEFORE cyber terrorists steal YOUR confidential information.

For the price of an iPad and a subscription cost less than most streaming video services, you can protect YOUR data from the vulnerabilities within the software systems/services you utilize every day.

TECHNICAL DETAILS

Feature	n@d@r
Identity application protocols (Facebook, YouTube, BitTorrent, etc.) in the network	✓
Record and Visualize hosts' historical application protocols usage	✓
Group hosts by VLAN, Operating System, Country, and Autonomous Systems	✓
Get a geographic map of your network communications with the rest of the world	✓
Identify top talkers (senders and receivers) hosts with minute resolution	✓
Visualize the top HTTP sites contacted by an host	✓
DLP via Fully Autonomous Detection & Response Mode	✓
Generate alerts when hosts cross ML time/traffic thresholds or have suspicious behaviors	✓
Get alerts notifications as Email, Discord, SMS, Webhook, Slack, Syslog messages	✓
Split, merge, and visualize VLAN based traffic	✓
Mobile Application* Command & Control	✓
Get a real-time view of top talkers and application protocols and compare them with daily activities	✓
Explore recorded nIndex (or SQL) data to review the cause of network problems	✓
Identifies top hosts, application protocols, countries, networks, and autonomous systems	✓
Custom Machine Learning Modes (Manual, Passive or Active)	✓
Unified Global Defense Neural Network* (UGDNN)	✓
Send alerts to ELK/SIEM/Splunk® Environments	✓
Query SNMP devices data, such as ACL, traffic and MAC address information	✓
Advanced Deployment Modes (Manual, Semi-Autonomous and Fully Autonomous	✓
Get total traffic and activity reports for any given host, network, or interface	✓
Identify attackers and victims through n@d@r dashboard in real-time and historical	✓
EDR Agent* on Windows, Linux & macOS	✓
Visualize host pools' historical applications protocols usage	✓
Continuous L3-L7 Network Traffic Analyzation (NTA)	✓
Leading Manufacturer Firewall Integrations*	✓
Advanced Diagnostic Insight via Node Isolation & Analysis	✓



To learn more about visit: https://us.nadar.ds-labs.dev/var

* Active DevOps Feature

DS Labs, LLC.
2336 SE Ocean Blvd, Suite 115
Stuart, FL 33996
info@us.nadar.ds-labs.dev

About DS Labs, LLC.

At DS Labs, our mission is to advance technologies that are driven by machine learning and provide organizations with scalable cloud-based platforms.

MITRE ATT&CK™ Breach & Attack Simulation