Radware Cybersecurity Alert

US Civilian Network Infrastructure Targeted by Pro-Russian Hacktivists

October 11, 2022

Following a series of DDoS attacks targeting government websites in the United States last week, Killnet's founder KillMilk, announced via an interview with Russia Today, that the threat group would target civilian network infrastructure in the United States over the coming days. Less than 48 hours later, pro-Russian hacktivist groups Killnet, NoName057(16), and Anonymous Russia began listing targets and announcing outages related to their DDoS attacks on websites of U.S. airports.

National Hacktivist

WHO IS KILLNET?

Killnet is a pro-Russian threat group known for launching denial-of-service attacks against those in public and private sectors that directly and indirectly support Ukraine or have in some way offended Russia. The group formed in January of 2022, selling DDoS services, but quickly transitioned into a hacktivist group following the Russian invasion of Ukraine.

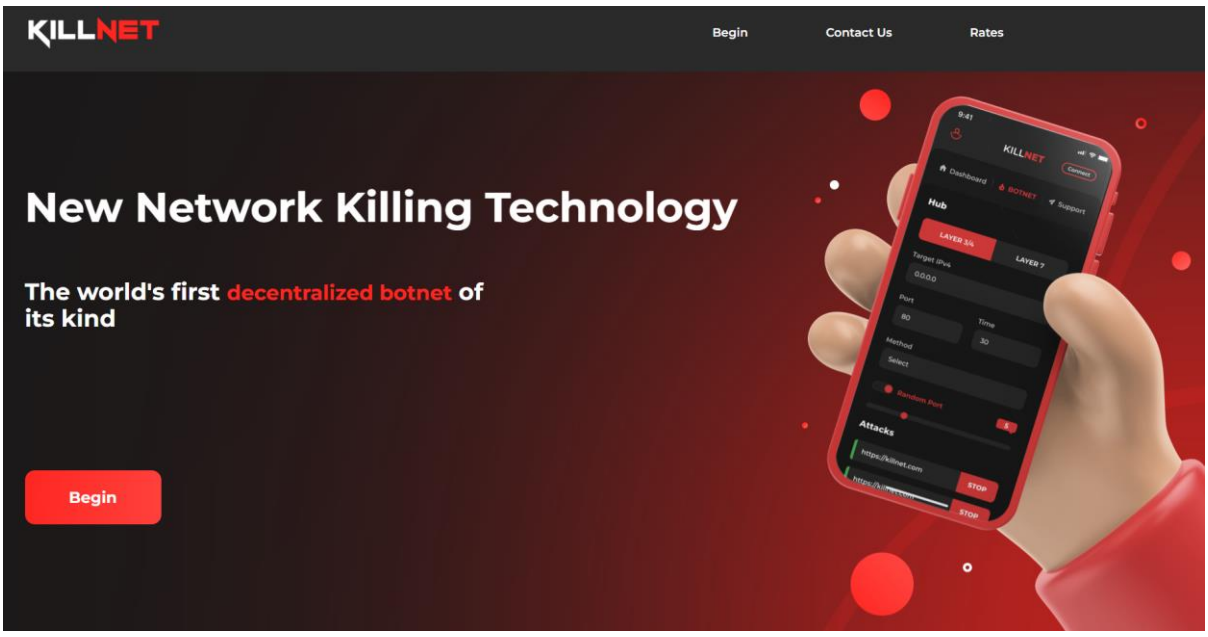

Figure 1: Killnet.io website advertising DDoS services (January 2022)

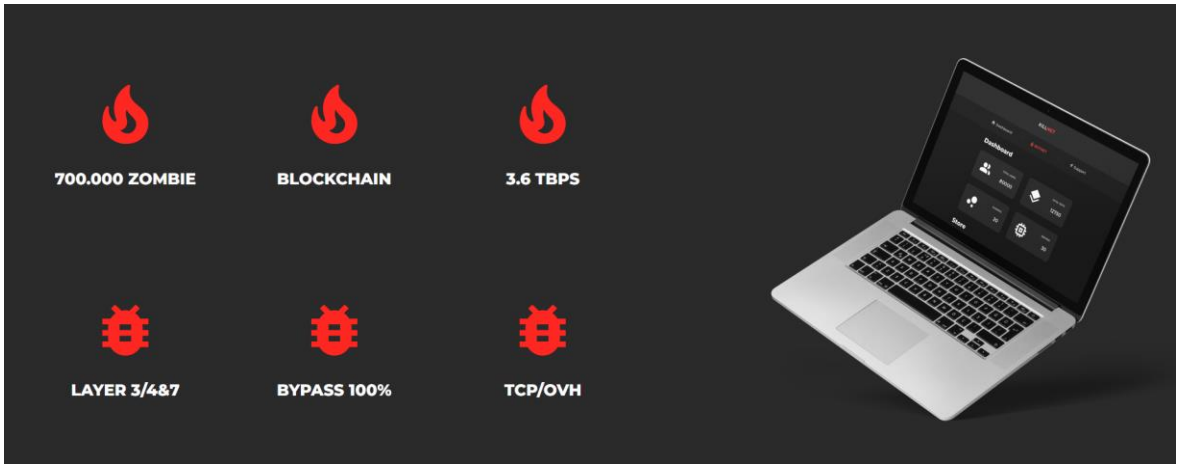

Figure 2: Killnet.io website advertising the Killnet botnet capabilities (January 2022)

Since the invasion, the group has gathered a following of nearly 100,000 subscribers on their main Telegram channel. KillMilk, the founder of the pro-Russian hacktivist group, claims that members of the group are ordinary people and denies any association with the Russian government. To maintain and grow their attack infrastructure, Killnet depends on donations.

WHO IS NONAME057(16) ?

NoName057(16) is a pro-Russian threat group known for launching defacement and DDoS attacks against Ukraine and those that directly and indirectly support Ukraine. The group formed in March of 2022 on Telegram and became a notable threat group by June. Since then, the group has gathered a following of nearly 13,000 subscribers. Noname057(16) has been seen operating in support of Killnet operations. At the time of publication, there is no evidence to suggest that NoName057(16) is working under the direction of the Russian government.

Demolish America's Name

On Sunday evening, October 9th, Russia Today published an interview with KillMilk, the founder of Killnet. KillMilk announced during the interview that Killnet is the "echo of future problems for the United States" and that the primary motivation for Killnet is to "repel the enemy." According to KillMilk, Killnet went through all their planned countries, and America will be their ultimate stand.

> *"THE UNITED STATES BRAGS ABOUT ITS CYBER TRAINING, BUT WHAT IT REALLY LOOKS LIKE AND HOW MUCH EXPERIENCE IT HAS IN CYBER WARFARE — YOU WILL SEE SOON THROUGH OUR ACTIONS. WE LEARNED AND BROKE EUROPE FOR EIGHT MONTHS WHILE THE UNITED STATES PREPARED TO CONFRONT US. WE ARE JUST BEGINNING TO CAUSE DISRUPTION IN AMERICA'S CYBERSPACE. KILLNET WILL ACHIEVE THE HIGHEST POSITION IN THE I.T. WORLD AND DEMOLISH AMERICA'S NAME BEFORE*

EVERYONE'S EYES. WHAT HAS BEEN HACKED NOW? IT'S TRIVIA. RATHER, ASK WHAT WILL HAPPEN NEXT WITH THE INFORMATION FIELD OF THE UNITED STATES."
– KILLMILK

KillMilk noted that he is a law-abiding citizen of the Russian Federation and does not get involved in the affairs of the Russian government, nor does he condemn their actions, adding that he does not commit crimes on the territory of his homeland.

Figure 3: KillMilk interview with Russia Today

In the same interview, KillMilk also **revealed** that Killnet is preparing a "huge package of evidence and revelations" that will implicate the United States in the creation of COVID-19.

DDoS Attacks Against the United States

US GOVERNMENT WEBSITES

On October 6th, the Governor's Office of Information Technology **announced** that the Colorado.gov state web portal homepage had resumed regular operation after a cybersecurity incident. While Colorado did not name the perpetrators, the pro-Russian hacktivist group Killnet claimed credit for the DDoS attacks that disrupted several government websites and included Check-Host links as proof of temporary disruption.

Figure 4: Message containing the list of attacked government websites (source, source)

Background: Check-Host (check-host[.]net) is an online tool for website monitoring and checking the availability of hosts, DNS records and IP addresses. It provides a capability to create permanent links to the check reports, leveraged by several denial-of-service actors to prove temporary disruptions or downtime. The nature of a denial-of-service attack is that the impact lasts only while the attack is ongoing, unlike wiping or crypto-locking attacks. Proving the success of such an attack can be tricky. Check-Host provides the necessary means to achieve this.

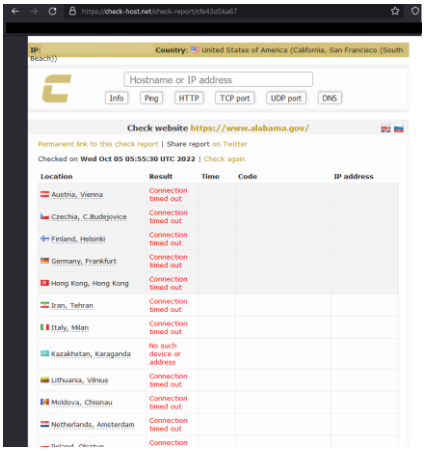

Figure 5: Check-Host report indicating disruption of Alabama.gov (source)

Radware Cybersecurity Alert

US Civilian Network Infrastructure Targeted by Pro-Russian Hacktivists

October 10, 2022

CIVILIAN NETWORK INFRASTRUCTURE

Early in the morning of October 10, one of the Killnet Telegram channels **announced** an operation to target civilian network infrastructure in the United States with coordinated DDoS attacks.

*Figure 6: Announcing DDoS attacks on US civilian network infrastructure (**source**)*

A few hours after the invitation to DDoS civilian network infrastructure in the United States, the **killnet_reservs** Telegram account published a **list** of airport websites in the United States and called on its members to launch targeted attacks against them. Seven minutes after killnet_reservs published the target list, threat group NoName057(16) posted an invitation link for people to join the Telegram channel **'DDosia Project**' and reposted the target list in that channel.

One hour after the target list was published by killnet_reservs and NoName057(16), the city of Chicago's air travel website, flychicago[.]com, was inaccessible. Following the outage in Chicago, Los Angeles International Airport (LAX), Hartsfield-Jackson Atlanta International Airport (ATL), and Phoenix Sky Harbor Airport (PHX) websites were all reported as offline.

Later in the day, Anonymous Russia posted a list of attacked airport websites with Check-Host report links.

Previous Attacks on Airport Websites

This is not the first time that these two threat groups have targeted airport websites. Killnet was listed in April 2022 in a CISA alert about Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure after launching a series of DDoS attacks against Bradley International Airport's website the month prior. Noname057(16) has also been observed launching DDoS attacks against airport websites in Poland, Estonia, and Lithuania.

Reasons for Concern

Threat groups Killnet and NoName057(16) present a moderate threat to the current landscape. While their Tactics, Techniques, and Procedures are considered low-level, these threat groups have recently demonstrated the ability to evolve into a more advanced threat.

It is important to note that denial-of-service attacks typically do not cause lasting damage. Still, those with unprotected assets or inadequate mitigation services may experience prolonged outages due to a DDoS attack from threat groups such as Killnet or NoName057(16). It is likely that the two threat groups will continue to target civilian network infrastructure over the next few months in the United States in an attempt to disrupt American lives and advance Russian propaganda.

EXPECTED TARGETS

- Transportation
- Marine and Shipping
- Healthcare
- Financial

Targeted Websites in October

US GOVERNMENT

- Gov2Go
- State of Alabama
- State of Alaska
- State of Colorado
- State of Connecticut
- State of Delaware
- State of Florida
- State of Hawaii
- State of Idaho
- State of Indiana
- State of Kansas
- State of Kentucky
- State of Mississippi

AIRPORTS

- Atlanta
- Alabama
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri

EFFECTIVE DDOS PROTECTION ESSENTIALS

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

LEARN MORE AT DDOS WARRIORS

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools visit **DDoSWarriors.com**. Created by Radware's **Emergency Response Team (ERT),** it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.