Radware Cybersecurity Advisory

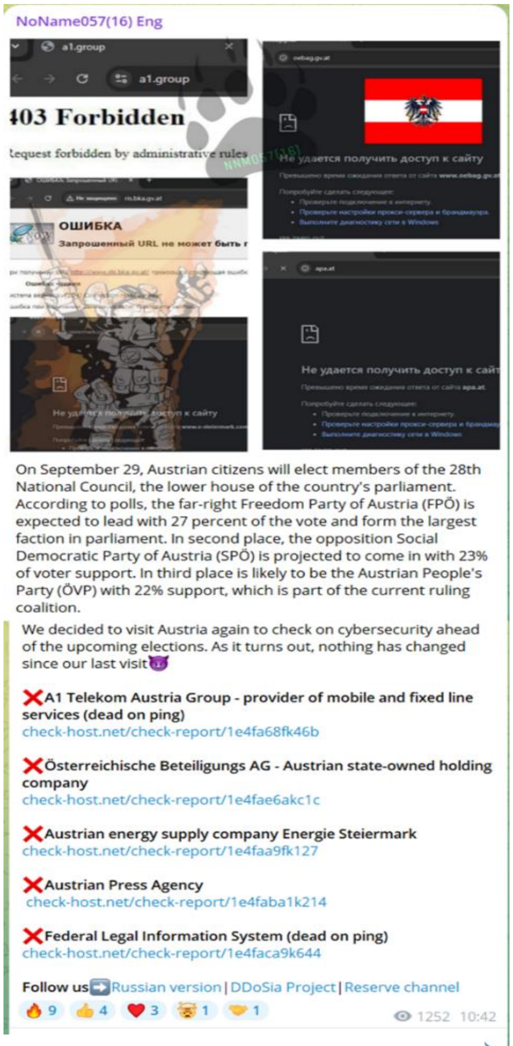
September 20, 2024

# Pro-Russian Hacktivists Target Organizations in Austria With DDoS Attack Campaign

*Threat groups launch a five-day—and counting—politically motivated cyberattack campaign that includes government sites, airports and the Vienna Stock Exchange.*

## Overview

- Pro-Russian threat actors NoName057(16) and OverFlame have launched a series of DDoS attacks on Austrian targets.
- The attacks are presumably connected to the Russian-Ukrainian conflict, although NoName057 claims they "decided to visit Austria again to check on cybersecurity ahead of the upcoming elections."
- The attack campaign started on September 16 and continues against over 40 targets including government sites, airports, financial services and Wiener Borse.


NoName057(16) Eng
a1.group
403 Forbidden
Request forbidden by administrative rules
ОШИБКА
Запрошенный URL не может быть
Не удается получить доступ к сайту
Не удается получить доступ к сайту

On September 29, Austrian citizens will elect members of the 28th National Council, the lower house of the country's parliament. According to polls, the far-right Freedom Party of Austria (FPÖ) is expected to lead with 27 percent of the vote and form the largest faction in parliament. In second place, the opposition Social Democratic Party of Austria (SPÖ) is projected to come in with 23% of voter support. In third place is likely to be the Austrian People's Party (ÖVP) with 22% support, which is part of the current ruling coalition.

We decided to visit Austria again to check on cybersecurity ahead of the upcoming elections. As it turns out, nothing has changed since our last visit😈

❌**A1 Telekom Austria Group - provider of mobile and fixed line services (dead on ping)**
check-host.net/check-report/1e4fa68fk46b

❌**Österreichische Beteiligungs AG - Austrian state-owned holding company**
check-host.net/check-report/1e4fae6akc1c

❌**Austrian energy supply company Energie Steiermark**
check-host.net/check-report/1e4faa9fk127

❌**Austrian Press Agency**
check-host.net/check-report/1e4faba1k214

❌**Federal Legal Information System (dead on ping)**
check-host.net/check-report/1e4faca9k644

**Follow us**➡️Russian version|DDoSia Project|Reserve channel

🔥 9 👍 4 ❤️ 3 1 1 1252 10:42

*Figure 1: NoName057 claims attacks on Austrian sites and provides the motivation through Telegram*

## Motivation

According to a NoName057 Telegram message, motivation is associated with the upcoming Austrian elections: "On September 29, Austrian citizens will elect members of the 28th National Council, the lower house of the country's parliament. According to polls, the far-right Freedom Party of Austria (FPÖ) is expected to lead with 27 percent of the vote and form the largest faction in parliament. In second place, the opposition Social Democratic Party of Austria (SPÖ) is projected to come in with 23% of voter support. In third place is likely to be the Austrian People's Party (ÖVP) with 22% support, which is part of the current ruling coalition. We decided to visit Austria again to check on cybersecurity ahead of the upcoming elections. As it turns out, nothing has changed since our last visit."

## Threat Actors

**NoName057(16)** is a pro-Russian hacker group known for its cyberattacks on Ukrainian, American and European websites of government agencies, media and private companies. It is regarded as a well-organized hacktivist group with over 2.5 years of experience targeting countries that support Ukraine or speak badly about Russia.

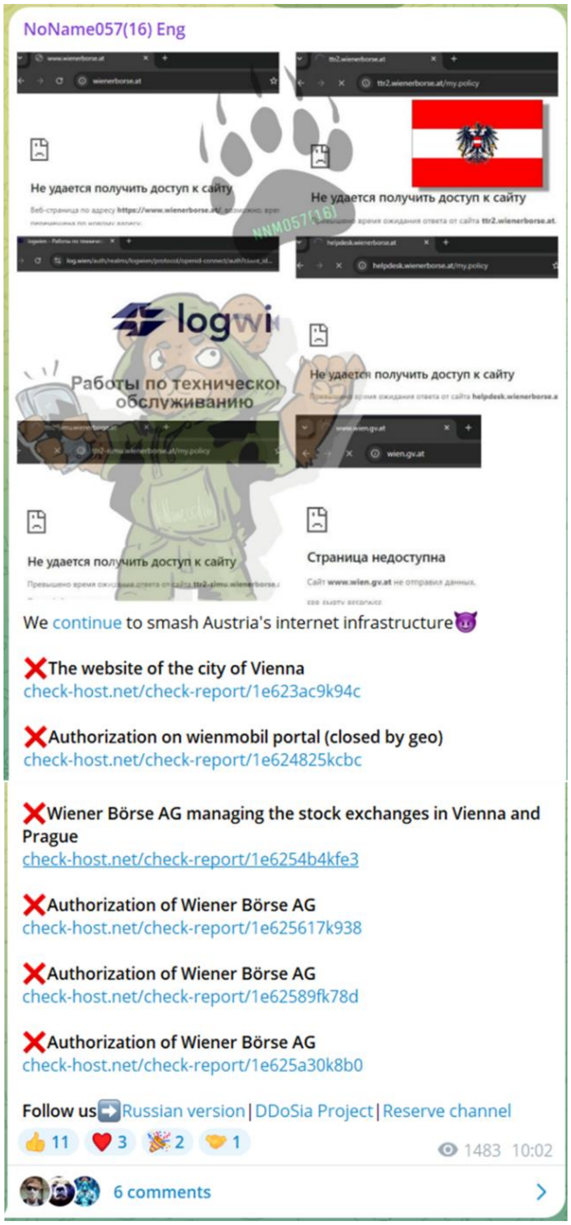
**OverFlame** is a relatively obscure hacktivist group known for targeting government institutions and corporations, particularly in Europe and North America. The group specializes in DDoS attacks and website defacements, often motivated by anti-government and anti-corporate sentiments. OverFlame operates through underground forums and encrypted messaging platforms, where they coordinate their attacks and recruit new members.

It is common to see like-minded threat actors make ad-hoc alliances and collaborate on campaigns to increase their impact.

## Attack Tools

Threat actors have mastered their ability to generate highly evasive and sophisticated HTTPS flood attacks that are hard to detect and mitigate.

The tool used by NoName057, the major threat actor in this campaign, is a crowdsourced botnet project named DDOSIA. The project leverages politically driven hacktivists willing to download and install a bot on their computers to launch denial-of-service attacks. Project DDOSIA, however, raises the stakes by providing financial incentives for the top contributors to successful denial-of-service attacks.


www.wienerborse.at
wienerborse.at
ttr2.wienerborse.at
ttr2.wienerborse.at/my.policy
Не удается получить доступ к сайту
Веб-страница по адресу https://www.wienerborse.at/ возможно, вре
Не удается получить доступ к сайту
Превышено время ожидания ответа от сайта ttr2.wienerborse.at.
NNM057(16)
helpdesk.wienerborse.at
helpdesk.wienerborse.at/my.policy
logwien
Работы по техническо
обслуживанию
Не удается получить доступ к сайту
Превышено время ожидания ответа от сайта helpdesk.wienerborse.a
ttr2-simu.wienerborse.at/my.policy
www.wien.gv.at
wien.gv.at
Не удается получить доступ к сайту
Превышено время ожидания ответа от сайта ttr2-simu.wienerborse.
Страница недоступна
Сайт www.wien.gv.at не отправил данных.

NoName057(16) Eng

We continue to smash Austria's internet infrastructure😈

❌The website of the city of Vienna
check-host.net/check-report/1e623ac9k94c

❌Authorization on wienmobil portal (closed by geo)
check-host.net/check-report/1e624825kcbc

❌Wiener Börse AG managing the stock exchanges in Vienna and Prague
check-host.net/check-report/1e6254b4kfe3

❌Authorization of Wiener Börse AG
check-host.net/check-report/1e625617k938

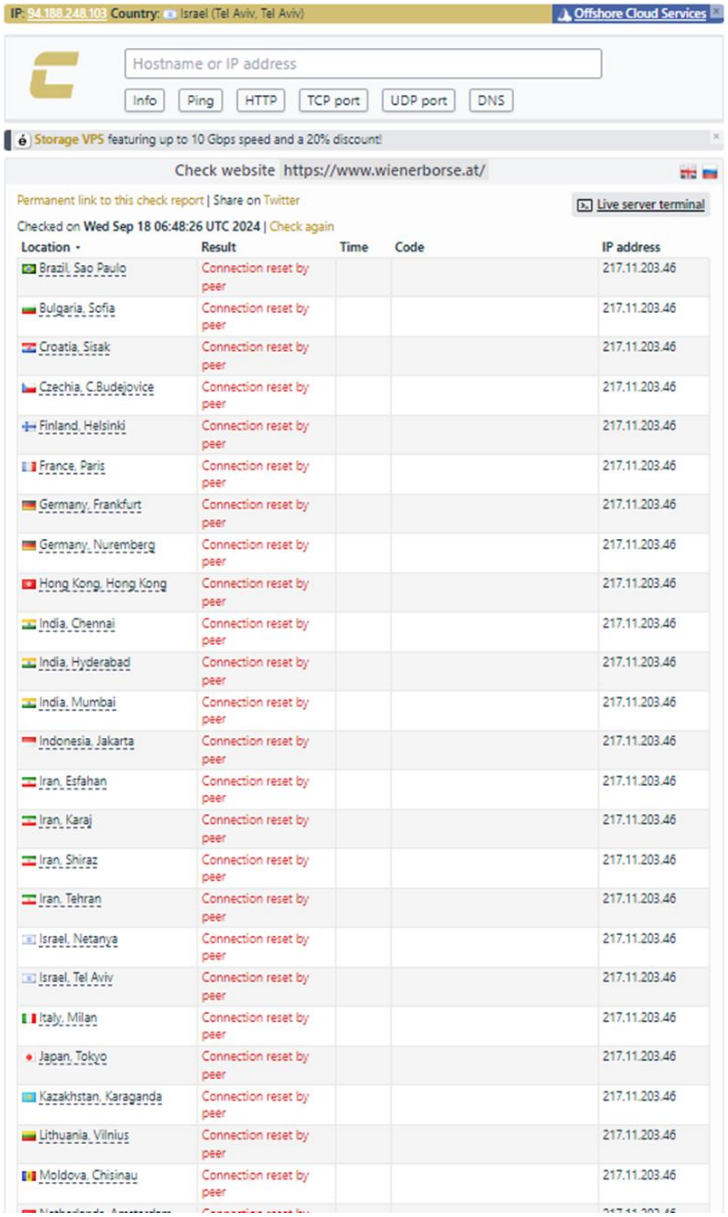
❌Authorization of Wiener Börse AG
check-host.net/check-report/1e62589fk78d

❌Authorization of Wiener Börse AG
check-host.net/check-report/1e625a30k8b0

Follow us➡️Russian version | DDoSia Project | Reserve channel

👍 11 ❤️ 3 🎉 2 🤝 1 👁 1483 10:02

6 comments



IP: 94.188.248.103 Country: Israel (Tel Aviv, Tel Aviv)

Storage VPS featuring up to 10 Gbps speed and a 20% discount!

Check website https://www.wienerborse.at/

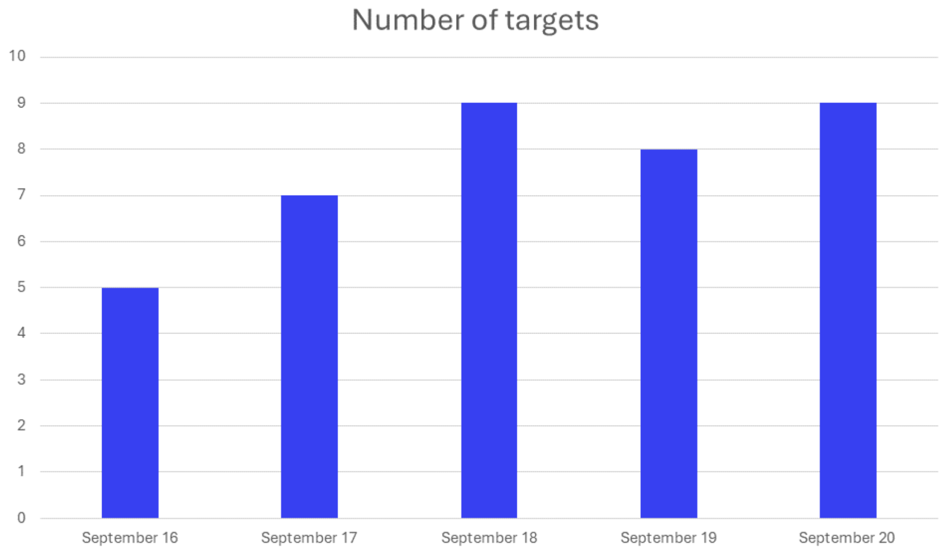
Permanent link to this check report | Share on Twitter

Checked on Wed Sep 18 06:48:26 UTC 2024 | Check again

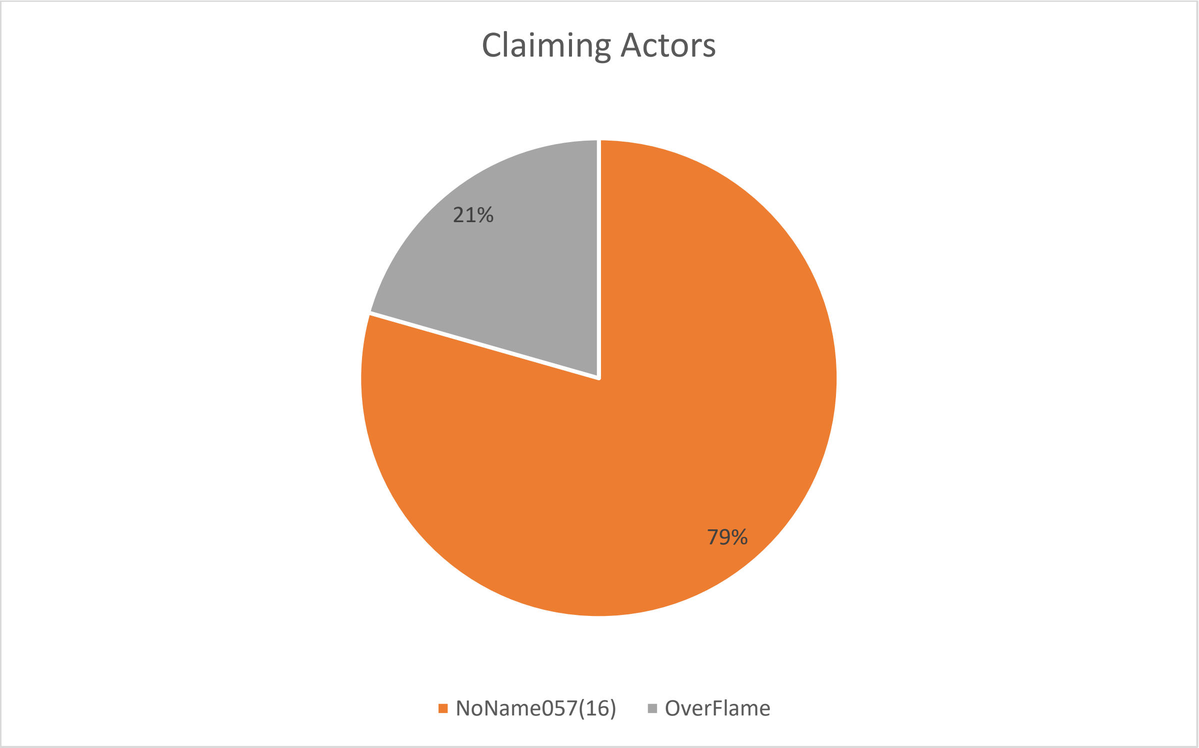
| Location | Result | Time | Code | IP address |
|---|---|---|---|---|
| Brazil, Sao Paulo | Connection reset by peer | | | 217.11.203.46 |
| Bulgaria, Sofia | Connection reset by peer | | | 217.11.203.46 |
| Croatia, Sisak | Connection reset by peer | | | 217.11.203.46 |
| Czechia, C.Budejovice | Connection reset by peer | | | 217.11.203.46 |
| Finland, Helsinki | Connection reset by peer | | | 217.11.203.46 |
| France, Paris | Connection reset by peer | | | 217.11.203.46 |
| Germany, Frankfurt | Connection reset by peer | | | 217.11.203.46 |
| Germany, Nuremberg | Connection reset by peer | | | 217.11.203.46 |
| Hong Kong, Hong Kong | Connection reset by peer | | | 217.11.203.46 |
| India, Chennai | Connection reset by peer | | | 217.11.203.46 |
| India, Hyderabad | Connection reset by peer | | | 217.11.203.46 |
| India, Mumbai | Connection reset by peer | | | 217.11.203.46 |
| Indonesia, Jakarta | Connection reset by peer | | | 217.11.203.46 |
| Iran, Esfahan | Connection reset by peer | | | 217.11.203.46 |
| Iran, Karaj | Connection reset by peer | | | 217.11.203.46 |
| Iran, Shiraz | Connection reset by peer | | | 217.11.203.46 |
| Iran, Tehran | Connection reset by peer | | | 217.11.203.46 |
| Israel, Netanya | Connection reset by peer | | | 217.11.203.46 |
| Israel, Tel Aviv | Connection reset by peer | | | 217.11.203.46 |
| Italy, Milan | Connection reset by peer | | | 217.11.203.46 |
| Japan, Tokyo | Connection reset by peer | | | 217.11.203.46 |
| Kazakhstan, Karaganda | Connection reset by peer | | | 217.11.203.46 |
| Lithuania, Vilnius | Connection reset by peer | | | 217.11.203.46 |
| Moldova, Chisinau | Connection reset by peer | | | 217.11.203.46 |
| Netherlands, Amsterdam | Connection reset by | | | 217.11.203.46 |

*Figure 2: NoName057 claims an HTTPS flood attack on the Wiener Boerse AG managing the stock exchange in Vienna and Prague. The Check Host page shows the victim resources were offline*

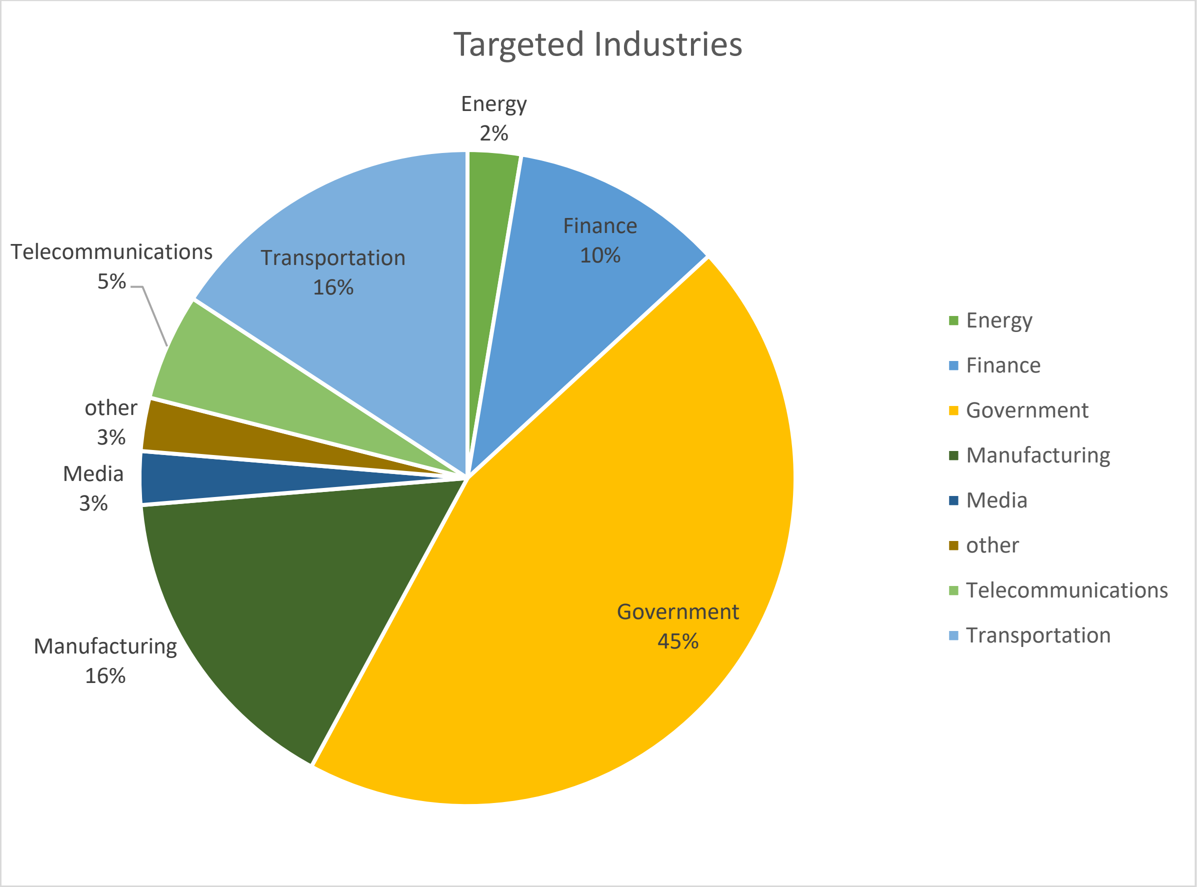
## Attack Timeline



## Claiming Actors



## Targeted Industries



## EFFECTIVE DDOS PROTECTION ESSENTIALS

**Behavioral-Based Detection –** Leverage Radware's advanced behavioral analysis to quickly and accurately identify and block anomalous bot activity while allowing legitimate traffic.

**Real-Time Signature Creation –** Utilize Radware's ability to promptly create and deploy signatures to protect against emerging threats and zero-day attacks.

**AI-Powered Content Analysis –** Implement Radware's AI-driven solutions to detect and mitigate sophisticated disinformation campaigns across multiple platforms.

**Cross-Platform Monitoring –** Employ Radware's comprehensive monitoring tools to track influence operations across various digital channels.

**Rapid Response Capabilities –** Leverage Radware's 24/7 Emergency Response Team to swiftly address and mitigate emerging threats.

For further network and application protection measures, Radware urges companies to inspect and patch their systems 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 achieve improved bot detection and blocking

**Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

**Flexible deployment options** including on-premises, out-of-path, virtual or cloud-based

## LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

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 Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED “AS IS” WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILBILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER’S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIREC, INCIDENTAL, CONSEQUENTIAL, OR EXAMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE**