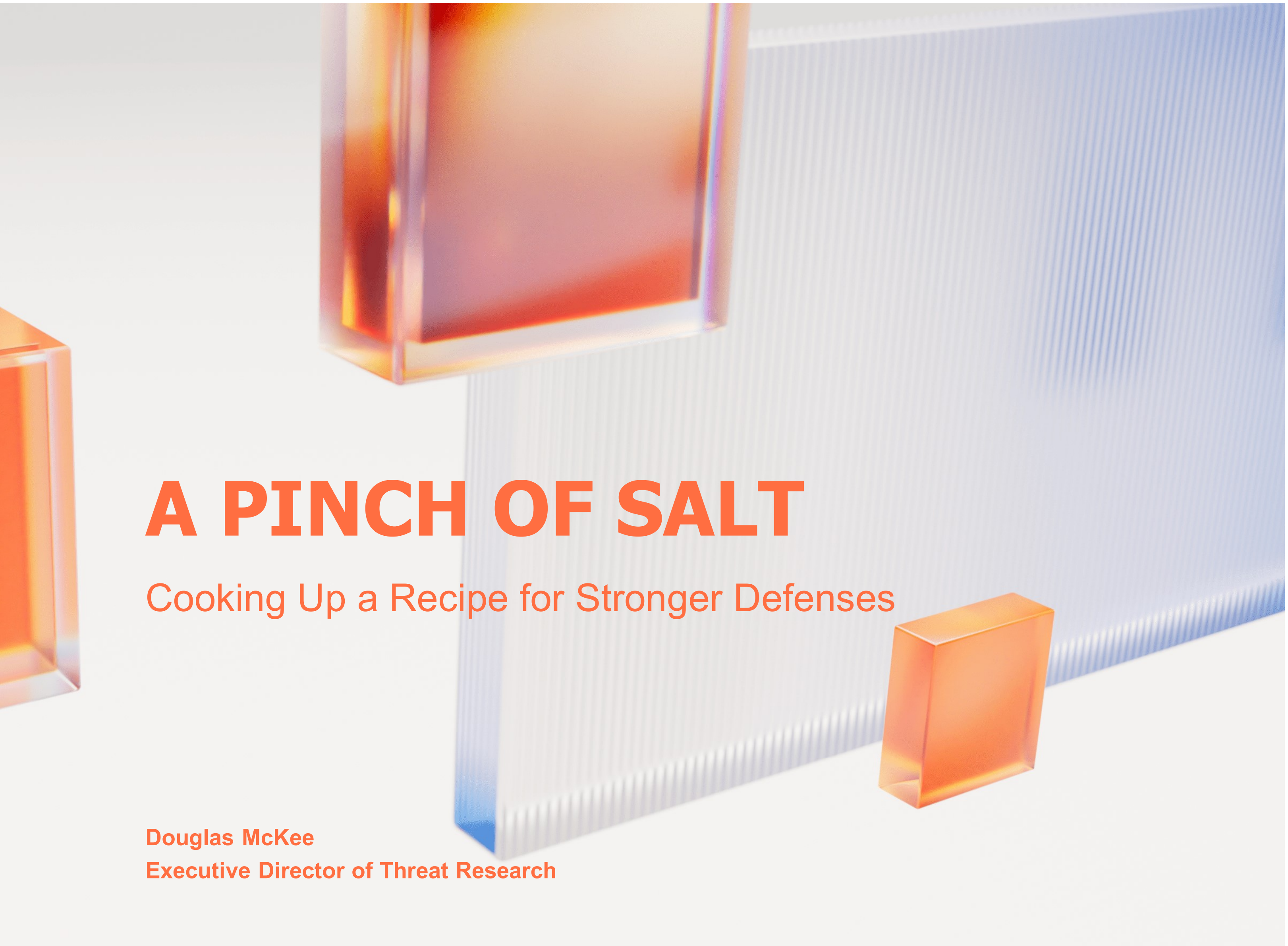
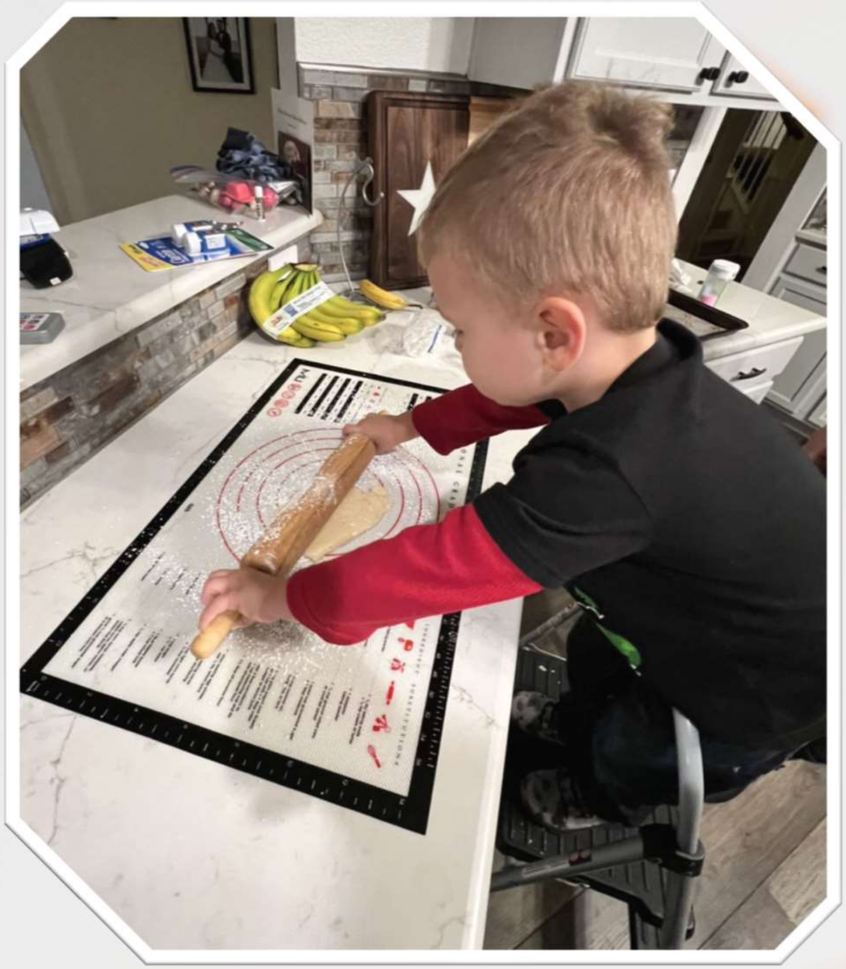


A PINCH OF SALT

Cooking Up a Recipe for Stronger Defenses

Douglas McKee
Executive Director of Threat Research

SONICWALL



WHAT ARE SOME OF YOUR FAVORITE FOODS?

Zach’s favorite foods

- Egg dishes and omelets
- Deli meat sandwiches
- Pizza
- Burritos and tacos
- Soups
- Chips, crackers, popcorn
- Pasta mixed dishes
- Cheeseburgers

IS SALT BAD FOR YOU?

Zach loves it!

It depends…

70%

“More than 70% of the sodium we consume comes from packaged, prepared and restaurant foods.”

*https://www.heart.org/

50%

“We typically consume about 50% more than recommended”

*https://www.heart.org/

75%

“An AHA survey found that about 75% of adults prefer less.”

*https://www.heart.org/

Understand the ingredients

8 BILLION

Intrusions detected on over 1 million sensors worldwide in 2024

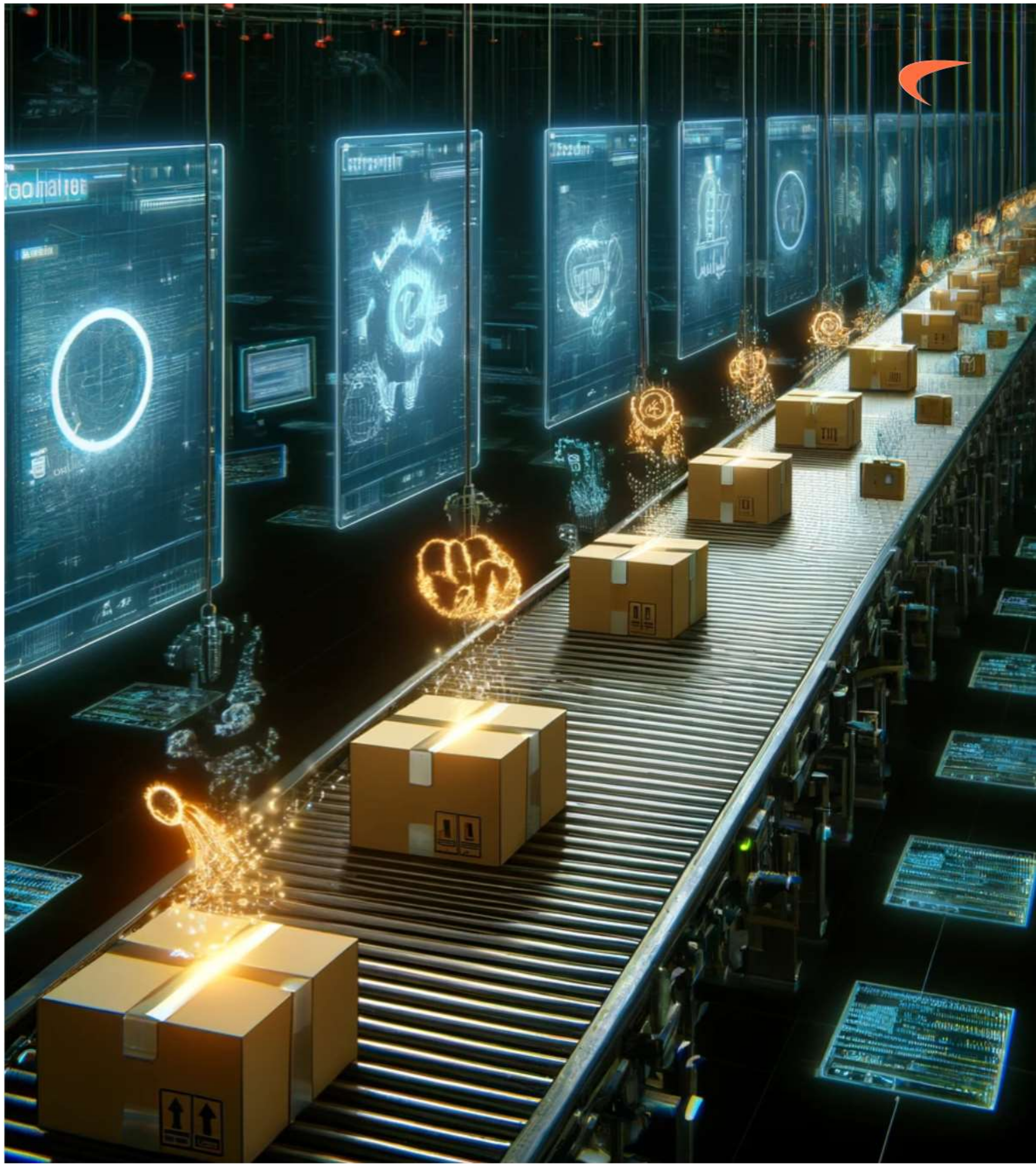
Data from 2024

What ingredients are the attackers using?

THE INGREDIENTS

Widespread Attackers love

- Log4j (CVE-2021-44228)
- Heartbleed (CVE-2014-0160)
- Shellshock (CVE-2014-6271)
- Apache Struts2 Remote Code Execution (CVE-2017-5638)
- Spring4Shell (CVE-2022-22965)



IS LOG4J BAD FOR YOU?

Attackers love it!

It depends!

It matters who is using the ingredients

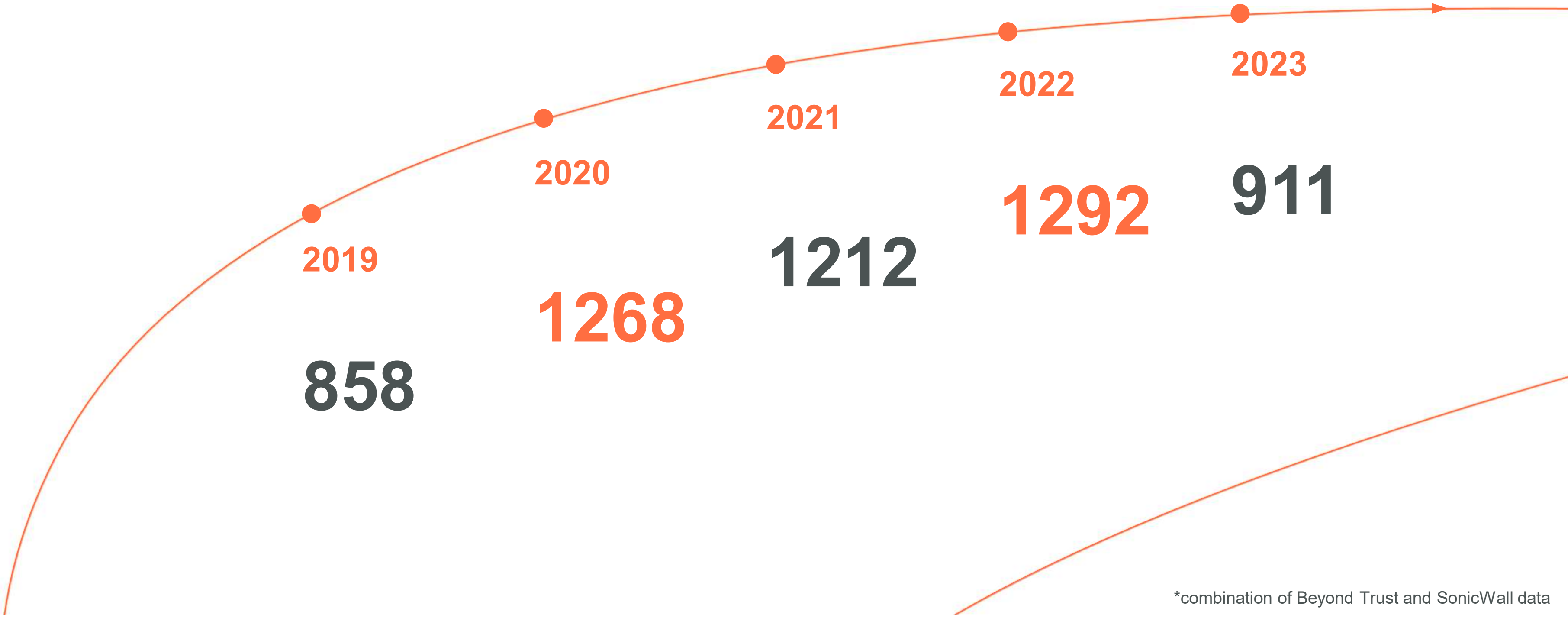
52%

of SMBs are affected by software supply chain vulnerabilities

Data from 2022-2024

MICROSOFT VULNERABILITIES

Total Per Year



2019	858
2020	1268
2021	1212
2022	1292
2023	911

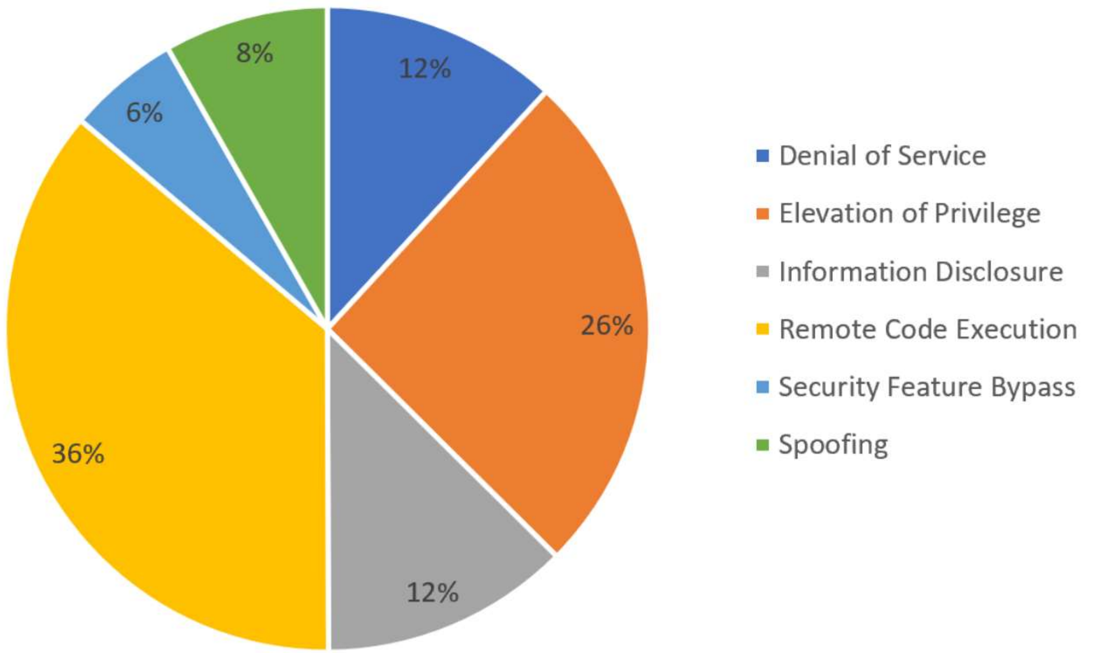
SONICWALL

*combination of Beyond Trust and SonicWall data

MICROSOFT 2023

Exploited Vulnerabilities By Type

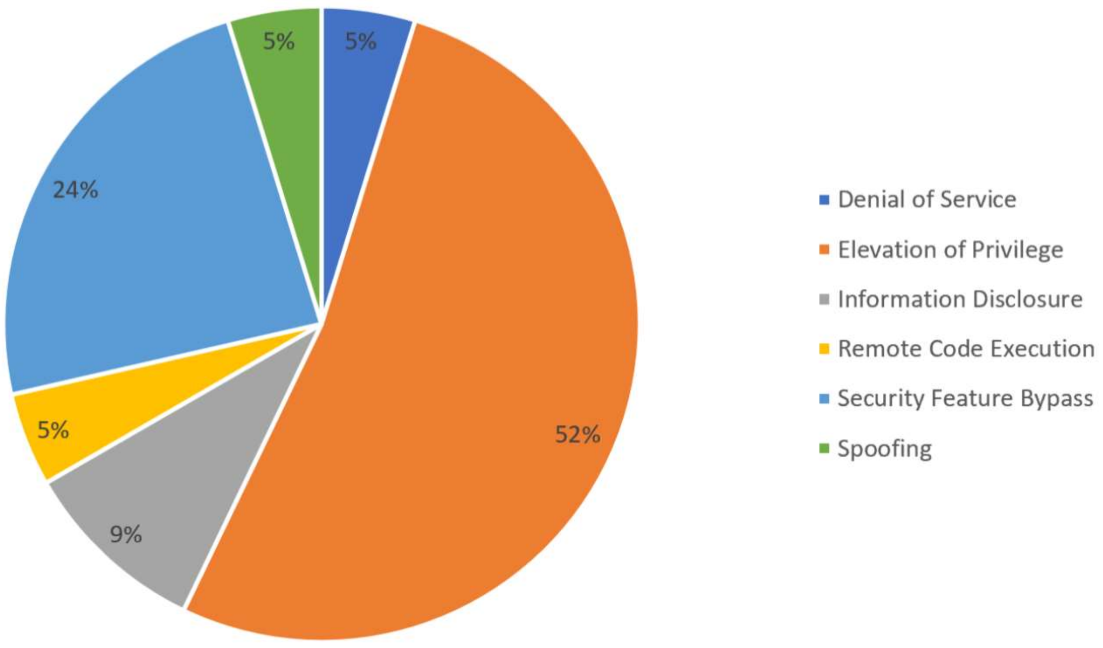
Remote Code Execution is most important?



MICROSOFT 2023

Exploited Vulnerabilities By Type

Attackers are using Elevation of Privilege the most against Microsoft Products



90%

Over 90% of prevalent malware families are leveraging PowerShell

Data from 2023

IS POWERSHELL BAD FOR YOU?

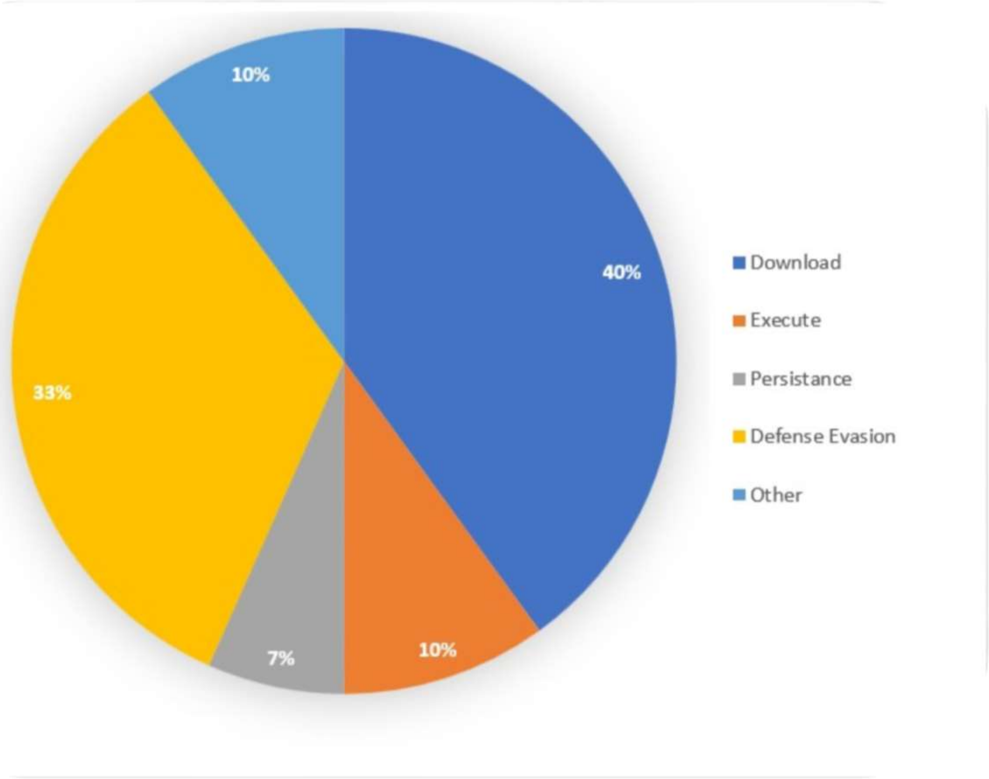
Attackers love it!

It depends!

POWERSHELL SINCE 2023

How is it being used?

Attackers are leveraging PowerShell mostly to download additional malware and evade defenses



100%

of SMBs would prefer less attacks

*Not real data

"Wisdom fortifies strength –
data empowers decisions."

Anonymous

OUTSIDE-IN APPROACH

Wisdom fortifies strength

1. Cybersecurity is a C-Suite issue
2. Infrequent alert monitoring
3. Different strokes for different folks

THE ART OF POSSIBLE

HOME > 2024 USA

Why Enterprise-Level Attacks Happen to SMBs - and How to Stop Them

Monday, May 6, 2024

2:20 PM - 3:10 PM PT

DATA EMPOWERS DECISIONS

Key takeaways from our threat data

Know Your Supply Chain Ingredients

Don't Ignore "Lower Impact" Vulnerabilities

Harden PowerShell

Image credit: Vecteezy.com

COOKING UP A RECIPE FOR STRONGER DEFENSES

1. Stay informed
2. Isolate - don't trust your dependencies
3. Leverage MSPs informed by threat data

SONICWALL®

Never alone.
Relentless security.