2019 Threats Predictions
McAfee Labs

**PowerShell In Memory**

2019 Threats Predictions

**Opening doors and connecting**

December 2018

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be
devices by password cracking
and exploiting vulnerabilities.

These alliances will flourish
to spur debate. Messages that perform best
cybercriminals will become
threats instead of just one.

Malware, exploits, botnets,
will actively work together.

One-Stop Attack

Bad actors are developing
advantage of phones and
control servers could
circumvent protections.

Cybercriminals can buy
sophistication can easily
on the underground
market. Criminals of
will become

malware-as-a-service families.

**Consolidation**

Evasion Techniques: The arm’s race continues to a new high

**Which Attack Is It?**

Simpler exploits will have
advantage in the Internet of Things
environments will continue to be a
profitable target for cybercriminals.

Social Media

As voice-controlled digital assistants are increasingly used to manage all

Focusing on one threat may
not be enough to detect
or remediate an attack.

Voice-Controlled Digital Assistants

New Entry to the Home

Speaking Aloud

As enterprises continue to fully adopt multiple cloud models (SaaS, PaaS, IaaS),

More Data to Steal

Large-scale identity platforms offer centralized secure authentication

and authorization of users, devices, and services across IT

environments—and a focus for criminals.

Identity Platforms and Edge Devices

Under Siege

Broken Trust

The IoT trust model is built on a weak

foundation of assumed trust and

perimeter-based security. Most IoT
tools are already common

circumvent protections.

**Data Exfiltration Attacks to Target the Cloud**

Script

Email

**Stopping One**

**Multifaceted**

Which Attack Is Not

category might miss the big

Ransomware as a smoke

Focusing on one threat may
not be enough to detect
or remediate an attack.

Data Exfiltration Attacks

More Data to Steal

Large-scale identity platforms offer centralized secure authentication

and authorization of users, devices, and services across IT

environments—and a focus for criminals.

Identity Platforms and Edge Devices

Under Siege

Broken Trust

The IoT trust model is built on a weak

foundation of assumed trust and

perimeter-based security. Most IoT
tools are already common

circumvent protections.

**Cybercriminals will become**

With amplification, the account gained 1,500

more followers in only four weeks by simply

One bot account with 279 followers, mostly

tweeting malicious content about their target.

**Evasion Techniques**

Evasion Techniques: The arm’s race continues to a new high

**Which Attack Is It?**

Simpler exploits will have
advantage in the Internet of Things
environments will continue to be a
profitable target for cybercriminals.

Social Media

As voice-controlled digital assistants are increasingly used to manage all

Focusing on one threat may
not be enough to detect
or remediate an attack.

Voice-Controlled Digital Assistants

New Entry to the Home

Speaking Aloud

As enterprises continue to fully adopt multiple cloud models (SaaS, PaaS, IaaS),

More Data to Steal

Large-scale identity platforms offer centralized secure authentication

and authorization of users, devices, and services across IT

environments—and a focus for criminals.

Identity Platforms and Edge Devices

Under Siege

Broken Trust

The IoT trust model is built on a weak

foundation of assumed trust and

perimeter-based security. Most IoT
tools are already common

circumvent protections.

**Data Exfiltration Attacks to Target the Cloud**

Script

Email

**Stopping One**

**Multifaceted**

Which Attack Is Not

category might miss the big

Ransomware as a smoke

Focusing on one threat may
not be enough to detect
or remediate an attack.

Data Exfiltration Attacks

More Data to Steal

Large-scale identity platforms offer centralized secure authentication

and authorization of users, devices, and services across IT

environments—and a focus for criminals.

Identity Platforms and Edge Devices

Under Siege

Broken Trust

The IoT trust model is built on a weak

foundation of assumed trust and

perimeter-based security. Most IoT
tools are already common

circumvent protections.

**Cybercriminals will become**

With amplification, the account gained 1,500

more followers in only four weeks by simply

One bot account with 279 followers, mostly

tweeting malicious content about their target.

**Evasion Techniques**

Evasion Techniques: The arm’s race continues to a new high

**Which Attack Is It?**

Simpler exploits will have
advantage in the Internet of Things
environments will continue to be a
profitable target for cybercriminals.

Social Media

As voice-controlled digital assistants are increasingly used to manage all

Focusing on one threat may
not be enough to detect
or remediate an attack.

Voice-Controlled Digital Assistants

New Entry to the Home

Speaking Aloud

As enterprises continue to fully adopt multiple cloud models (SaaS, PaaS, IaaS),

More Data to Steal

Large-scale identity platforms offer centralized secure authentication

and authorization of users, devices, and services across IT

environments—and a focus for criminals.

Identity Platforms and Edge Devices

Under Siege

Broken Trust

The IoT trust model is built on a weak

foundation of assumed trust and

perimeter-based security. Most IoT
tools are already common

circumvent protections.

**Data Exfiltration Attacks to Target the Cloud**

Script

Email

**Stopping One**

**Multifaceted**

Which Attack Is Not

category might miss the big

Ransomware as a smoke

Focusing on one threat may
not be enough to detect
or remediate an attack.

Data Exfiltration Attacks

More Data to Steal

Large-scale identity platforms offer centralized secure authentication

and authorization of users, devices, and services across IT

environments—and a focus for criminals.

Identity Platforms and Edge Devices

Under Siege

Broken Trust

The IoT trust model is built on a weak

foundation of assumed trust and

perimeter-based security. Most IoT
tools are already common

circumvent protections.