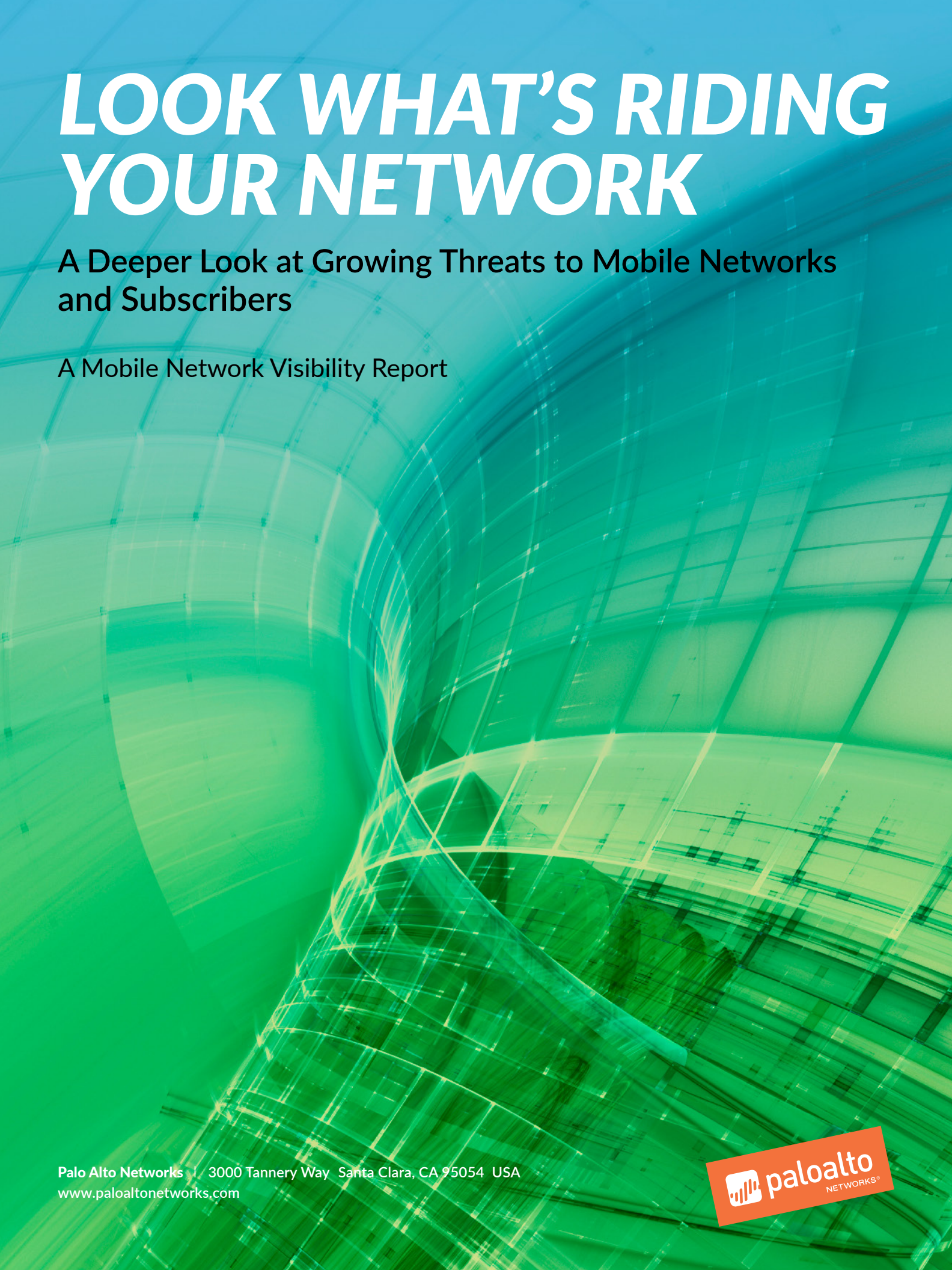
LOOK WHAT'S RIDING YOUR NETWORK

A Deeper Look at Growing Threats to Mobile Networks and Subscribers

A Mobile Network Visibility Report



Palo Alto Networks | 3000 Tannery Way Santa Clara, CA 95054 USA
www.paloaltonetworks.com

paloalto NETWORKS®

Do you know what threats are riding your network?

Where are they coming from? Who will they impact? How many devices are already infected?

As the digital experience increasingly moves to mobile devices, so do the cyber activities of malicious actors. Android-based malware threats continue to grow while Android-based devices escalate in quantity, IoT adoption expands, and mobile traffic grows exponentially. Infected devices are not only a threat to subscribers — they can be recruited into botnets to attack mobile network infrastructure and damage service availability. Evidence of these threats can be found in service provider networks.

Operators are faced with the difficult challenge of separating out the hidden quantities of malicious traffic from massive volumes of mobile data that they transport to determine which threats can be ignored and which compel action. Given the rapidly evolving threat landscape and operator cost pressures to increase revenue and migrate to next-generation networks, this is an enormous challenge indeed.

Will the threat landscape for mobile networks and devices reach the attack volume witnessed with Windows® devices and enterprise networks? We believe the answer is "yes," and this report provides compelling evidence that the trend is well underway, drawing from multiple research and analysis sources:

- Palo Alto Networks®, Unit 42 threat research
- Trillions of data points from WildFire® cloud-based threat analysis service
- Analysis of traffic samples from service provider and enterprise networks
- Experience and input with more than 45,000 global security customers and partners

Mobile network operators need to be fully informed about what threats are riding their network, where they coming from and who is impacted in order to make credible decisions and take appropriate action to protect their networks and subscribers.

As the security industry leader, Palo Alto Networks provides the Next-Generation Security Platform that enables full visibility and context across all mobile network domains.

The new reality is that threat vectors are opportunistic, dynamic and designed to expand reach by probing and exposing both old and new technology vulnerabilities which can only be effectively mitigated through automated visibility techniques."

– Heavy Reading, "The Evolution of Securing: Harnessing the Power of Automated Visibility"

The mobile industry is growing rapidly – mobile malware is growing even faster.

With 57,000 new Android-based subscriptions added every hour, cybercriminals have a rapidly expanding base of potential victims.

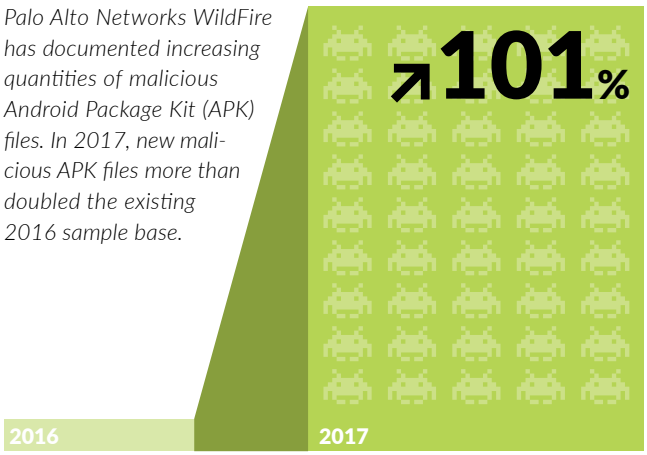
In 2017, on average, cybercriminals generated 10 new malicious APK for every 1,200 new Android-based smartphone subscriptions added by the mobile industry.

In 2017, global mobile subscriptions reached a total of 7.8 billion. By 2023, more than 30 billion connected devices are forecast, including 20 billion IoT devices.

Cybercriminals have taken note of this massive growth and have turned their malicious activity toward mobile and IoT devices and networks, as well as accelerated their development of Android-based malware. As almost 90 percent of new mobile devices sold are Android-based, and as there are more vulnerabilities in the ecosystem, it is the favorite target for malicious actors.

Mobile Malware Growth

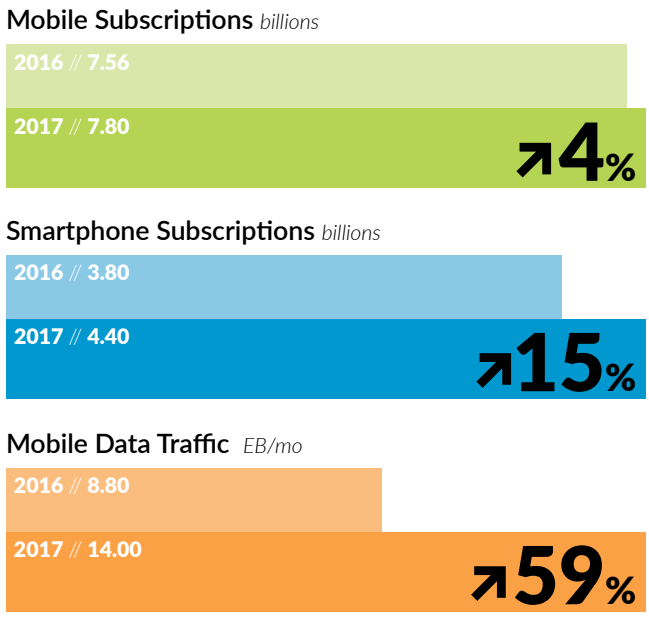
Palo Alto Networks WildFire has documented increasing quantities of malicious Android Package Kit (APK) files. In 2017, new malicious APK files more than doubled the existing 2016 sample base.



WildFire Total malicious APK Sample Base

**APK files are analogous to other software packages such as APPX in Microsoft Windows.*

Mobile Industry Growth



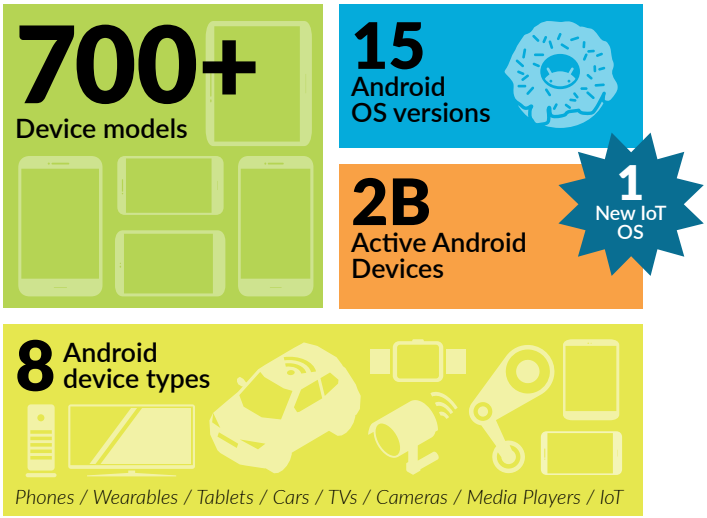
Source: Ericsson Mobility Report, November 2017

Mobile subscriptions, including all devices, operating systems and network technologies, have grown steadily at 2-4 percent over the past decade and are expected to continue at 4 percent through 2022. Smartphone subscriptions and mobile data traffic has been growing even faster at 15 and 59 percent respectively.

The mobile industry added an estimated 42 million Android-based smartphone subscriptions every month – that's 57,000 every hour.

The security challenges of the Android ecosystem — more options but greater vulnerability

Android® is the most popular mobile operating system, used by 80+ manufacturers, in more than 700 models and more than half a dozen types of devices other than mobile phones.



as of May 2017

One Billion

Outdated Devices

More than half of the 2 billion active Android devices have OS software that is more than two years old.

- Fragmentation of the Android ecosystem, including the wide diversity of devices, OS versions and manufacturers, makes device-based protection difficult to enforce and complex to administer.
- Android OS will continue to expand to new types of devices, such as IoT.

Unsuspecting Victims With Vulnerable Devices

The large majority of malicious APKs were delivered to unsuspecting victims via simple web downloads.

Android Package Kit is the package file format used by the Android operating system for distribution and installation of mobile apps and middleware. APK is the primary method used by malicious actors to infect mobile devices, including IoT devices.

Every hour, hundreds of new malicious APK files are discovered by WildFire.

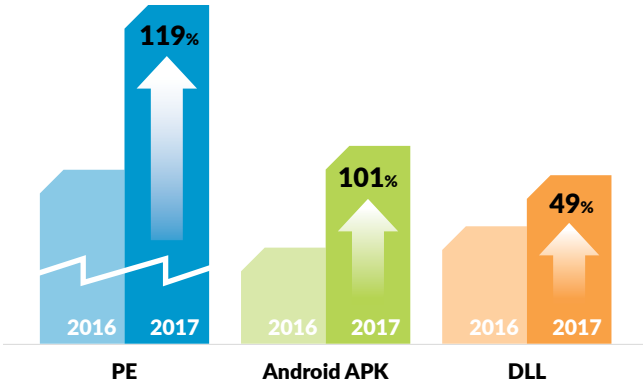
New malicious APK files are created by malicious actors in an attempt to bypass existing protections.

Millions of malicious APK files have been documented over the last few years and, once documented, are routinely blocked by Palo Alto Networks Next-Generation Security Platform.

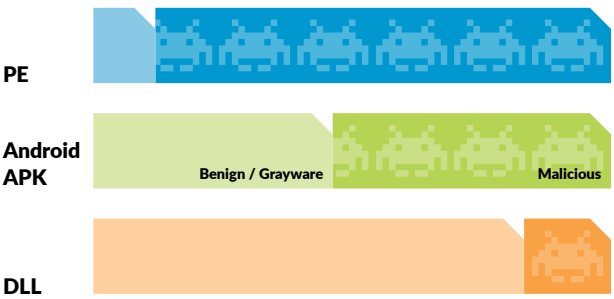
APK is overtaking other file types used by cybercriminals for malicious activity.

In just two years, APK-delivered malware has grown 30-fold and now comprises a significant percentage of all malicious file samples in the WildFire database.

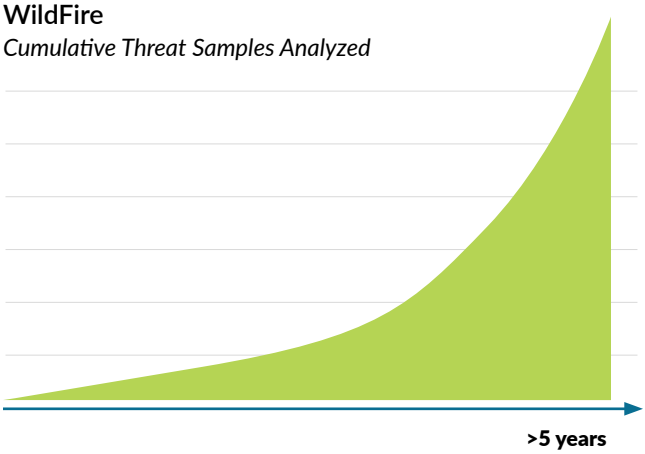
Annual Growth in New Malicious Files %



WildFire Samples *by Verdict*



WildFire
Cumulative Threat Samples Analyzed



Historically, windows-based file types — Dynamic Link Library and Portable Executable — DLL and PE — dominated the volume of malware found. In 2017, new malicious APK files surpassed DLL files in volume to become the second-most prevalent malicious file type collected in 2017.

This recent surge in new malicious APK files indicates the increased focus cybercriminals are now taking on mobile targets and underscores the need for stronger, automated security in mobile networks.

Malicious APK File Samples Have Doubled in Volume

In 2017, new APK files became the second-fastest-growing malicious file type, doubling the total volume of APKs and edging past new malicious DLL samples. The volume of new malicious APKs is now approaching the growth rates of malicious PE files. Since 2015, WildFire has recorded 30-fold increases in malicious APK. In 2017, tens of thousands of new malicious APK files were uncovered every day through WildFire.

APK Files Are More Likely to be Malicious

In 2017, out of millions of new APK file samples analyzed, almost half were found to be malicious — far exceeding the malicious frequency of most other file types examined.

Trillions of High-Quality Data Points

Palo Alto Networks WildFire has collected and analyzed billions of submitted samples from service providers, enterprises, governments and third parties to identify malicious files, malware and other threats, as well as provide automated preventions. In addition to PE, DLL, and APK files, file types analyzed include Microsoft® Word, PDF, PE64, DLL64, Microsoft Excel®, Adobe® Flash®, RTF, ELF, RAR Archive, Microsoft PowerPoint® and others.

As mobile traffic increases exponentially, malicious activity is increasingly difficult to isolate, identify and protect against.

Malicious activities are hidden in exabytes of data carried by service provider networks and can rapidly infect millions of mobile devices.

Cybercriminals hide in the huge volumes of traffic that mobile network operators must process. As mobile usage continues to increase year over year and cybercriminals use automation to instantly create malware modifications, the task of finding malicious traffic has become increasingly difficult.

In 2017, WildFire analyzed billions of traffic samples from service providers and enterprise and deemed millions to be malicious. Hidden malicious files in a mobile network are the source of most malicious cyber activity, including those triggering high-volume DDoS attacks.

Finding that malicious traffic in the terabytes of data an operator transports needs to be the primary objective of service provider network security strategies.

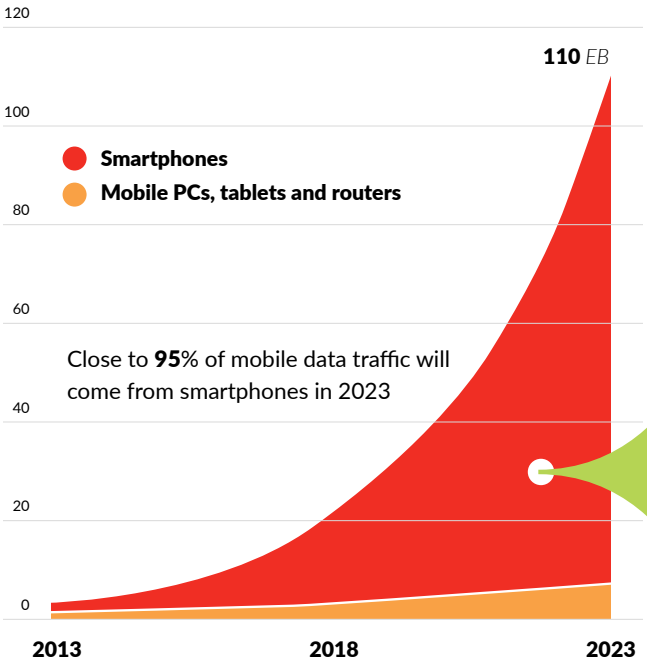
For service providers, high performance and throughput are critical criteria in infrastructure equipment decisions. A successful security posture must comb through exabytes of traffic and billions of mobile and IoT devices to accurately and rapidly identify traffic attempting to infect devices as well as those devices already infected.

Rapid Spread of Malware Instances

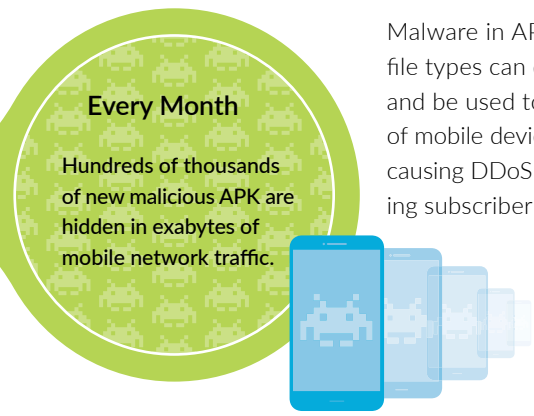
New malware can spread exponentially once it is introduced.

A typical malicious APK file can be as small as 5Kb, making it difficult to find. WildFire threat analysis service has witnessed malware spreading to more than 45,000 separate instances in just 30 minutes. Clearly, if left unchecked, malware could quickly spread throughout a mobile network or the IoT and other networks it manages.

Global mobile data traffic *Exabytes per month*



Source: Ericsson Mobility Report 2017



Malware in APKs and other file types can quickly spread and be used to infect millions of mobile devices in a network, causing DDoS attacks or invading subscriber confidentiality.

At least 18,000 malicious zombie domains can be accessed through unmaintained mobile apps.

Originally published through legitimate sources, zombie C2 will easily pass an antivirus check.

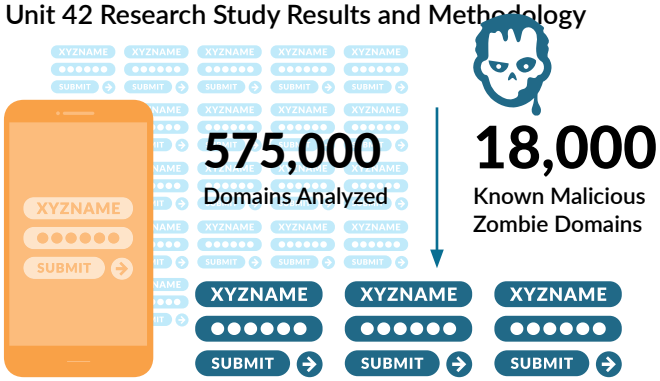
A "zombie C2" is an unmaintained C2 channel: A mobile app usually maintains one or multiple command-and-control, or C2, channels with remote master servers. Since 2008, a great number of Android mobile app and SDK companies have failed, leaving their SDK and C2 channels unmaintained and their domain names for command-and-control available to register at a cheap price. Those unmaintained C2 channels are the "zombie C2" channels.

Easily passes antivirus check: An adversary taking over a zombie C2 channel can easily influence all APK files connected to it. Since the zombie C2 and the APK files are usually legitimate and have been published for a long time, they will easily pass an antivirus check.

Converts apps into malware: Research by Unit 42 on a huge data set shows that the zombie C2 channels phenomenon exists widely with great potential security risks. In two attack demos, if the adversaries can take control of those zombie C2 channels, they can easily convert legitimate apps into powerful malware.

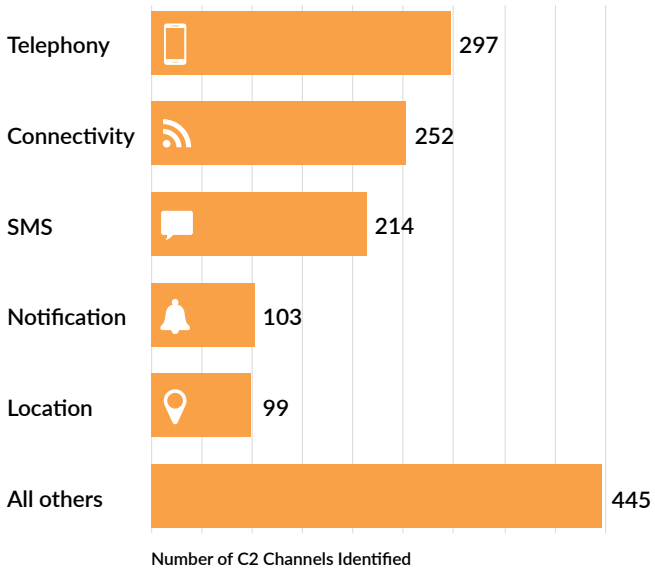
Great security risk: With well over half of Android devices having outdated OS, there is great opportunity for cybercriminals to leverage zombie domains for malicious purposes.

Unit 42 Research Study Results and Methodology



- 65,000 zombie domains — 18k malicious; 47k legitimate
- 33,000 zombie domains easily available through domain registration to malicious adversaries
- 30,000 established legitimate C2 channels available to adversaries
- 2,984 established malicious C2 channels available for reuse

Top sensitive system services used by malicious zombie C2 clients



The top sensitive services are very similar in both malicious and legitimate zombie C2. Both are interested in knowing the current system status, app installation status, network status and location services. Also, they are interested in SMS services, camera services and even command executions. The legitimate zombie C2 channels contain as great security risks as malicious ones.

Most Common Dangerous Behaviors:

The zombie C2, once appropriated for malicious purposes, can utilize standard permissions to conduct the following activities:

- Collect the privacy information from users (e.g., IMEI, IMSI, device type, screen size, fine-grained location)
- Steal the incoming SMS messages
- Automatically download apps and promote users to install them — could be used by large-scale malware distribution
- Load specified URL and show it to users, i.e., a phishing webpage.

Source: Palo Alto Networks Unit 42, "**Beware! Zombies are Coming**"

Malware that threatens network infrastructure is readily found in networks observed.

Service provider networks are vulnerable to both mobile and non-mobile malware.

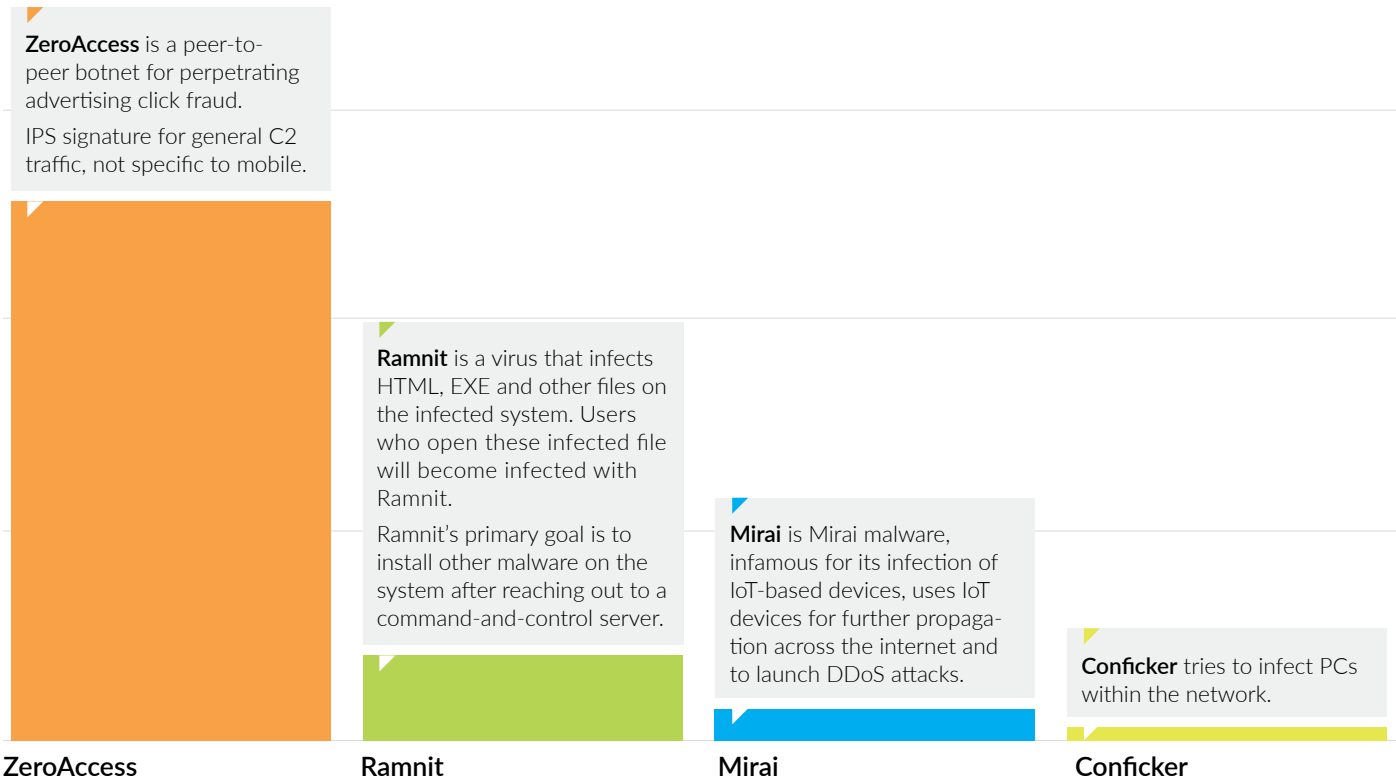
Malicious actors can attack mobile infrastructure as well as network transport elements such as transport, OSS/BSS systems and IT infrastructure. These examples illustrate the types of threats found in service provider networks.

Attackers can rapidly infect large numbers of lightly protected smart, mobile and IoT devices, and leverage them as botnets — threatening both the mobile infrastructure and the subscriber or enterprise customer. Bots are often embedded in those mobile and IoT devices without users or "things" even being aware of them. Infected non-mobile devices can be turned toward transport infrastructure to seriously impair performance.

About a month after the infamous Mirai attack in late 2016, the same malware took a more evolved tactic by targeting a specific vulnerability in a management interface present in routers used by almost a million customers of a Tier 1 operator, with the goal of infecting the devices and making them part of the Mirai botnet. The infection attempts failed but nevertheless caused the routers to crash.

Notable Malware Threats Discovered Example Service Provider Networks	
Service Provider A	**Service Provider B**
Conficker	ZeroAccess
Pushdo	Ramnit
Dorkbot	Mirai
SLocker	Conficker

Example Service Provider *Sample count per 1 million subs*



Ransomware and silent SMS can severely impact subscribers.

While some types of malware on consumer devices are simply nuisances, more serious threats should not be ignored.

Subscribers Unknowingly Install Malicious APKs

Android malware requires user interaction for an APK to be loaded onto a mobile device. Adversaries have to resort to social engineering to lure the user into taking multiple steps to install unknown APK files, such as asking the user to "Allow APKs from unknown source," and requiring the user to confirm installation as well as permissions to read specific data during installation.

Ransomware Has Moved to Android

Ransomware has quickly become one of the greatest cyberthreats facing organizations around the world. Cybercriminals have perfected the key components of these attacks, leading to an explosion of new malware families, more effective techniques and new malicious actors.

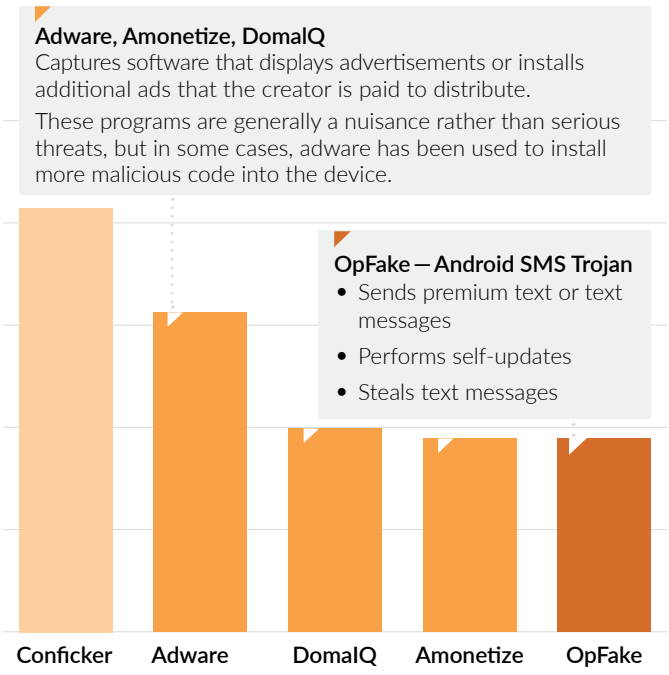
Ransomware is a lucrative business with little or low-cost barriers to entry. It has begun expanding attacks to platforms outside of Windows, such as Android phones, via third-party APK files that are loaded with user interaction. Any device that an attacker can hold for ransom will be a target in the future.

The ransomware business model can be easily applied to the "Internet of Things" (IoT). For example, after infecting the refrigerator, the attacker could remotely disable the cooling system and only re-enable it after the victim has made a small payment.

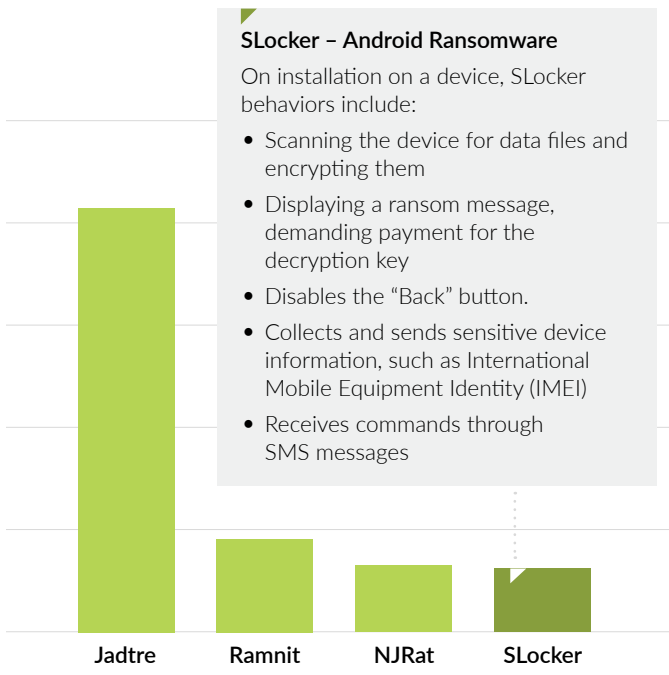
Source: Unit 42, "RANSOMWARE: UNLOCKING THE LUCRATIVE CRIMINAL BUSINESS MODEL

Notable Malware Threats Observed Example Service Provider Networks	
Service Provider C	Service Provider D
Conficker	Jadtre
Adware	NJRat
DomaIQ	Ramnit
Amonetize	SLocker
OpFake	Adware

Example Service Provider *Sample count per 1 million subs*

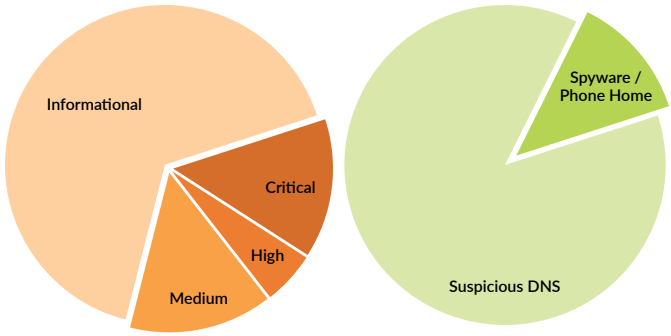


Example Service Provider *Sample count per 1 million subs*

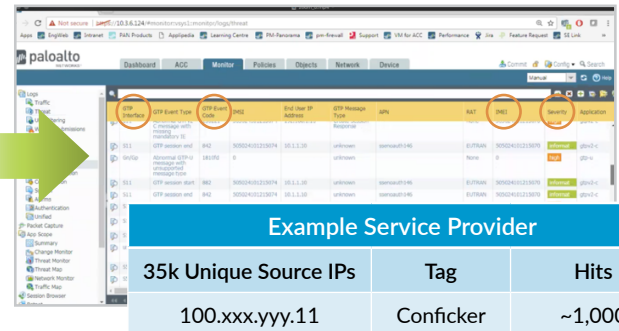


Deep visibility into command-and-control activity reveals threat severity and impact.

Full visibility identifies impacted network elements, devices and subscribers, and helps prevent future botnet attacks.



Example Service Provider *Sample count per 1 million subs*



Example Service Provider		
35k Unique Source IPs	**Tag**	**Hits**
100.xxx.yyy.11	Conficker	~1,000
100.xxx.yyy.12	Conficker	~1,000
100.xxx.yyy.13	Vinute	<10
100.xxx.yyy.14	Conficker	~1,000

Discover the Threat and Where It Is Located

Large volumes of traffic to suspicious or known malicious destinations indicate existing malware infection of network elements, IoT or subscriber devices. Operators can observe this activity through security systems at the DNS, internet (S/Gi), RAN, roaming or other mobile network peering points, depending upon network architecture and operator preferences. Events can be reported and categorized by severity and flagged for further analysis.

In many cases, events catalogued are informational only, such as nuisance or lower priority malware. Other more critical threats can be flagged for further analysis and investigation. For example, C2 activity originating from network elements or high-value enterprise or IoT customers may warrant deeper analysis.

In the example shown here, the service provider noted more than 250,000 C2 events accessing suspicious domains or known spyware in one week.

Analyze Who or What Is Affected

With deep traffic inspection of signaling and data, combined with application-layer visibility, operators can detect and analyze malicious activity to determine whether it threatens the network or subscribers. Further identification of destination and source IP address or IMSI/IMEI can isolate which devices or elements are affected and the volume at risk. In one service provider network examined, more than 35,000 unique IP addresses communicated with known malicious domains. These were all subscriber devices, not network elements. Knowing what subscribers are impacted can help determine the appropriate action or notification to take.

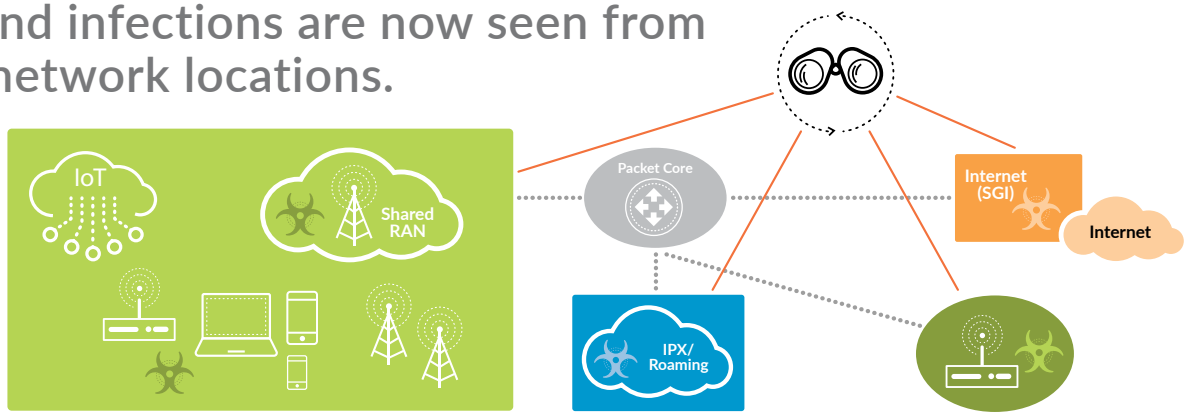
Prevent and Protect

Armed with full visibility, mobile network operators can make more effective policy and prevention decisions, such as blocking communication to known malicious sites or blacklisting DoS generating endpoints.

Subscribers' unknowingly install malicious files and contribute toward botnet-initiated DDoS. Identification of infected devices, notification to subscribers, blocking of C2 activity and prevention education can help protect network availability.

Complete network visibility — across all network domains, signaling and data planes — impacting the network and subscribers.

Attacks and infections are now seen from multiple network locations.



		Threat to Network Availability	Threat to Subscriber	Low Severity / Information
S/Gi (Internet)		**Malicious Domains and Malware** • Inbound from internet — phishing, trojan. Lure personnel to penetrate infrastructure security • Outbound C&C from Infected devices	**Malicious Domains and Malware** • Inbound from internet — phishing, trojan. Lure subscribers to download malware or visit other malicious sites. • Outbound C2 from infected devices	**Adware, Amonetize, DomalQ** • Displays advertisements or installs additional ads that the creator is paid to distribute • Generally a nuisance rather than a serious threat, but in some cases, adware has been used to install more malicious code into the device.
RAN		**Infected IoT Devices** • Botnet-enabled DDoS • Mirai, Conficker, Ramnit (non-mobile) **Signaling Vulnerabilities** • SCTP or other signaling flood • Local outage • Non-malicious floods	**Ransomware and Silent SMS** • Once infected, C2 communication is established and ransom is demanded. • SLocker, Locky, OpFake • Impact: increase calls to customer care	
Roaming		**GTP Vulnerabilities** • Roaming partner or infected roaming devices • Abnormal packets • GTP signaling flood • Local outage		
Non-3GPP		• Infected devices can attack network elements.	**Non-Mobile Threats** • Mobile devices can be infected through unprotected Wi-Fi. • Cross-platform infection • Mirai, Conficker, Ramnit	

Threats are no longer limited to just the internet (S/Gi) interface. With a large and growing base of smartphones and IoT devices largely uncontrolled by the operator, threats to the network can come through the RAN, roaming partners or even non-3GPP peering points, such as Wi-Fi. Analysis of mobile network operator traffic has uncovered malware, command-and-control activity, and access to malicious domains. Some of these target the subscribers, including annoying adware as well as devastating ransomware. Others target network infrastructure and can cause outages or other service disruption. Some anomalies that can cripple network availability are caused by unintentional, non-malicious actions or outage events.

Palo Alto Networks

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, maintaining trust in the digital age by helping tens of thousands of organizations worldwide, including service providers, enterprises and government agencies, prevent cyber breaches. With our deep cybersecurity expertise, commitment to innovation, and game-changing Next-Generation Security Platform, service providers can confidently pursue a digital-first strategy and embark on new technology initiatives, such as cloud, NFV and mobility.

https://www.paloaltonetworks.com/company

Methodology

Data and analysis in this report was derived through Palo Alto Networks threat and analysis resources, including the WildFire threat database, Unit 42 threat research, AutoFocus database, summary data from live network trials and other industry research. Industry sources consulted also include the Ericsson Mobility Report 2017 and the Nokia 2017 Threat Intelligence Report

Test Your Network

To request a free Security Lifecycle Review of your network, please visit:

https://get.info.paloaltonetworks.com/webApp/security-lifecycle-review-risk-assessment-en

The WildFire database has collected and analyzed billions of submitted samples from service providers, enterprises, governments and third parties to identify malicious files and other threats, and provide automated preventions.

Every mobile network is unique, and the examples shown in this report are not necessarily representative of all mobile networks or averages of the entire mobile industry.

The Palo Alto Networks Next-Generation Security Platform for mobile network operators provides automated, application-layer visibility, prevention and enforcement across all peering points in the mobile network. Advanced GTP features correlate threat data to subscriber and device identifiers, providing easily accessible and actionable information. Operators can determine when and where threats enter the network and which devices or subscribers are impacted to take appropriate enforcement action.

WildFire cloud-based threat analysis is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The cloud-based service employs a unique multi-technique approach that combines dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.