WEBROOT®
Smarter Cybersecurity™

+

AIRLOCK®
SECURE ACCESS HUB

2019 Webroot

THREAT REPORT

MID-YEAR UPDATE

SEPTEMBER 2019

WHAT'S INSIDE

INTRODUCTION

The act of prediction, itself, is the application of probability to determine what might happen. For example, if a person takes an action once, you might expect them to do it again. However, if that action caused a poor or negative result, you'd most likely expect the person not to do it again. Now, let's make it more complex. Say that the person has taken the action in some situations, but not in others. By analyzing the details of each situation, determining the differences and factors in each one, you could begin to predict the likelihood of the person's actions in a given context. Thus, to make a reasonable prediction for the future, you must have clear insight into past events, complete with context.

In essence, that is what Webroot strives to do with threat intelligence. By examining internet data and objects to determine threat trends, we can calculate the probability of future threat behavior. As millions of websites, domains, and IP addresses change state from benign to malicious and back, we can analyze trends and map the relationships between them, as well as with other internet objects, such as files and applications. This, in turn, allows us to better predict the potential for benign websites and IPs to turn malicious and vice versa, and even predict where future attacks may originate.

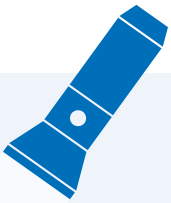
Upon examining our threat intelligence data from the first half of 2019, it's fairly clear the trends we've observed over the last several years are still going strong. In particular, we've continued to see increases in polymorphism, phishing, and attack innovation overall.

This mid-year update to the annual Webroot Threat Report showcases data from the Webroot® Platform, our advanced machine learning-based threat analysis architecture, as well as trends, insights, and predictions from the Webroot Threat Research Team.

CHANGES IN ENDPOINT MALWARE

In general, one of the bigger trends we've seen in malware is a shift to more reconnaissance. While attackers are still launching numerous malware campaigns, we've observed that criminals are performing more recon upfront to determine the value a system could give them. For instance, if they detect a system or network of systems with excellent speed and processing power, they might choose to launch an attack that would use those systems to mine cryptocurrency. Alternatively, if they breach an endpoint device that has connections to a much wider network of critical infrastructure, they might launch ransomware to encrypt business-critical systems and extort money from their victims.

> *Although a high number of infections is still valuable, threat actors are effectively going for quality over quantity when they choose to profile their victim's worth.*
>
> – Jason Davison, Advanced Threat Research Analyst



THREAT SPOTLIGHT:

DANABOT AND ITS EVOLUTION

Given the recent dominance ransomware has had in the malware scene, hearing about a good old-fashioned banking Trojan delivered via phishing email may sound like a blast from the past. But, as cybercriminals are always shifting tactics to evade detection and increase their likelihood of success, it makes sense that they might bring back an old favorite and then build on it.

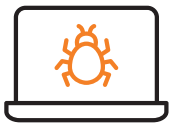
A Trojan called DanaBot was first offered for sale on a semi-private forum in April of 2018. Armed with basic Trojan and info stealing functionality, DanaBot works to gather sensitive banking information from unsuspecting users for fraud and other criminal activity. While these activities, in themselves, are nothing new, this Trojan has continued to evolve.

In particular, DanaBot has added affiliates, increased its geotargeting, and expanded its functionality overall to include new modules, such as a proxy module (used for injects), a stealer module, and a Tor module. It's even expanded to deliver ransomware.

OF MALWARE IS UNIQUE TO A SINGLE PC.

Overall, malware encounter rates remained relatively flat with the numbers from 2018, but there are a couple important things to note. First, our data shows that 95% of malware samples we've encountered are unique to a single machine, up from 92% last year. That means nearly all of today's threats are polymorphic, making it more or less impossible to detect them by signature-based technologies.

Second, although malware infection numbers didn't change significantly, there were notable shifts when looking at Windows® versions being infected, as well as the geographic locations of the infected devices. Examining the data side by side, it's likely that the increase in infections affecting the Middle East, Asia, and Africa correlate with the use of older or unpatched operating systems.



PERCENTAGE OF MALWARE SAMPLES ENCOUNTERED ON WEBROOT-PROTECTED PCS

1 PC	95.2%
2-100 PCS	3.9%
11-100 PCs	0.8%
101-500 PCs	0.12%
501-1000 PCs	0.01%

PERCENTAGE OF INFECTED WINDOWS® DEVICES BY REGION

Middle East	11.0%
Asia	10.1%
Africa	8.8%
South America	8.0%
Europe	4.4%
North America	3.2%
Australia/NZ	2.5%
Japan	2.2%
UK	2.3%
Other	2.8%

WEBROOT-PROTECTED DEVICES, BY OPERATING SYSTEM AND REGION

	Windows® 8 and older	Windows® 10
Middle East	53%	47%
Asia	49%	51%
Africa	51%	49%
South America	39%	61%
Europe	45%	55%
North America	34%	66%
Australia/NZ	43%	57%
Japan	56%	44%
UK	44%	56%
Other	50%	50%

Third, we've seen an uptick in malware attacking older operating systems. When compared with 2018, malware targeting Windows® 7 machines has risen 71%. In general, computers using the Windows 7 operating system are twice as likely to become infected as those running Windows® 10, with approximately .12 infections per Windows 7 device so far in 2019, and 0.05 infections per Windows 10 device.

Finally, out of all the malware seen, home user PCs continue to be nearly twice as likely to become infected as business PCs (64% and 36% respectively). There are a variety of contributors to this discrepancy, not least of which is that most corporate devices are protected by business firewalls and mandatory security, while home users may be more lax in protecting their devices. Second, the average person is more likely to exercise caution while browsing the web on a work device that their employer owns.[1]

76% OF ALL MALWARE HIDES IN ONE OF THREE PLACES ON A WINDOWS® SYSTEM.

PRO TIP

For businesses, creating Windows® policies to prevent execution from %temp% and %cache% could prevent a number of threats from successfully infecting a given endpoint device.

MALWARE TARGETING WINDOWS® 7 SYSTEMS HAS RISEN 71%

> *"Even though older operating systems are being used less and less, breaching even a single out-of-date machine can take down a company's whole network. That's how infections like WannaCry and NotPetya spread so quickly in 2017—they took advantage of vulnerabilities in older, unpatched operating systems."*
>
> – Briana Butler,
> Sr. Engineering Data Analyst

[1] Webroot Inc. "Hook, Line and Sinker: Why Phishing Attacks Work." (September 2019)

EXPERT INSIGHT: MALWARE TRENDS

Jason Davison, advanced threat research analyst at Webroot, gives a summary of his observations of the malware ecosystem so far in 2019.

1

MONKEY SEE, MONKEY DO.

Less sophisticated threat actors attempt to watch and mimic successful strategies used by the larger more organized groups.

2

MORE DATA, MORE PROBLEMS.

The larger, more organized threat actors have a big data problem on their hands. Having a plethora of infections means having to efficiently and effectively sift through all that information to determine which infections are valuable enough to pursue.

3

IT'S JUST BUSINESS.

After determining which attacks have the greatest success rate and profitability, criminals can target entire networks through lateral movement and privilege escalation before deploying their ransomware payload. They intentionally target victims that cannot afford to shut down, such as schools, state governments and departments, and hospitals. If attacked, these organizations generally have no choice but to pay, unless they have secure backups in place.

PREDICTION

"I expect that the efficiency surrounding major, organized threat operation will continue to improve. I believe there's already a fair amount of automation on their end, and we're likely to see more of that, particularly in terms of lateral movement and jumping from one high-value target to the next."

JASON DAVISON, ADVANCED THREAT RESEARCH ANALYST

URL AND IP-BASED THREATS

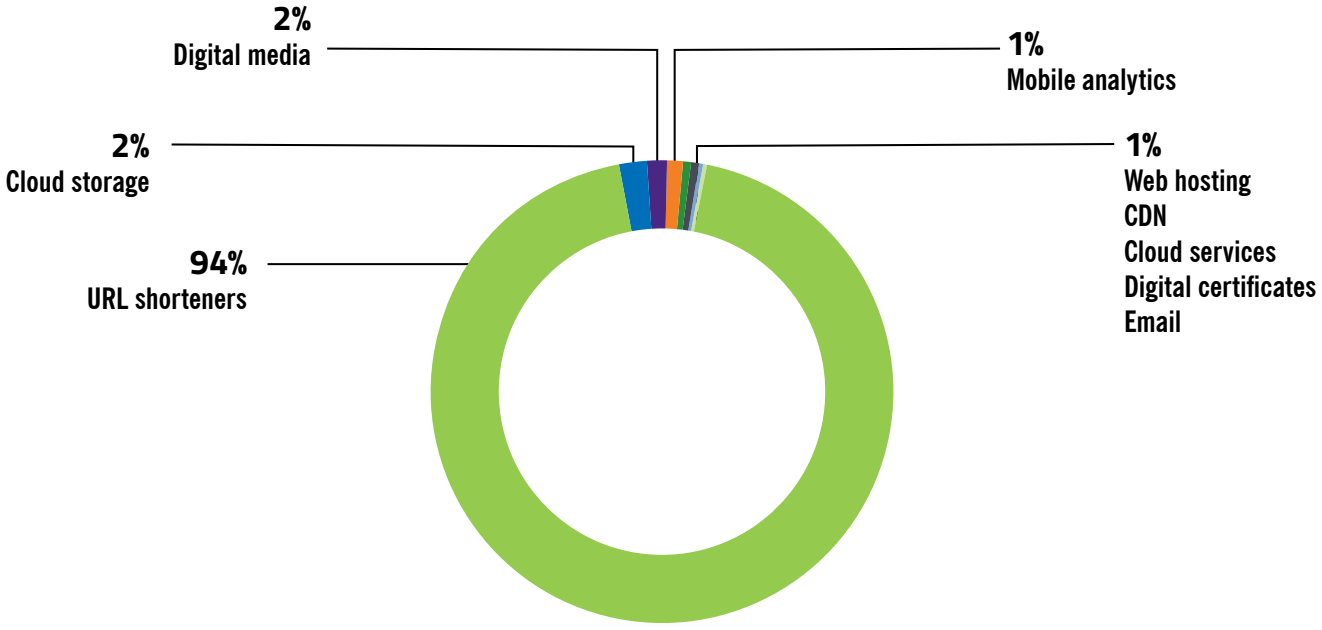
1 IN 4 MALICIOUS URLs WERE FOUND HOSTED ON TRUSTED DOMAINS.

With increasing frequency, cybercriminals are doing whatever they can to take advantage of trust. So far in 2019, nearly 1 in 4 malicious URLs (24%) were found on trusted domains. Criminals hijack pages on legitimate sites to host malicious content, knowing that it's more difficult for security measures to block URLs on these domains, and that end users are less likely to be suspicious of pages on domains they recognize. We saw much of this behavior across 9 distinct domain content categories (of the top 1,000 most popular domains), including URL shorteners (bit.ly, TinyURL, tiny.cc, etc.), cloud storage (Dropbox, SharePoint, Google™ Drive, etc.), and digital media (Tumblr, Imgur, etc.).

While malicious URLs are very dynamic and change frequently, the total number we've encountered has remained relatively flat compared with previous years' data, constituting about 2% of all websites in existence.

1 IN 50 URLs IS MALICIOUS

In itself, that number may not sound terribly impressive, but it actually represents a significant risk. In essence, 1 in 50 URLs is malicious. When you think about the number of links you click or websites you visit each day, you can begin to appreciate the amount risk there really is. In fact, 85% of people worldwide admit to clicking up to 50 work-related links, as well as up to 50 personal life-related links, in an average day.[2]



[2] Webroot Inc. "Hook, Line and Sinker: Why Phishing Attacks Work." (September 2019)

THREAT SPOTLIGHT:

CRYPTOJACKING, NEITHER FORGOTTEN NOR GONE

Cryptojacking refers to the practice of using browser-based programs that run via scripts embedded in web content to mine cryptocurrency with unused CPU without the user's knowledge or consent.

The originator of the first recorded cryptojacking script, CoinHive, shut down on March 8, 2019. However, numerous copycats have emerged, including DeepMiner, DeepMinerAnonymous, JSECoin, CryptoLoot, CoinImp, and others.

Although browser-based security measures are improving to thwart this threat, it's not going away any time soon. Currently, there are over 87,000 domains hosting cryptojacking scripts, according to our detections. In fact, this number hit an all-time high in July, during which Webroot blocked just over 1 million URL requests to pages hosting cryptojacking scripts.

EXPERT INSIGHT

Tyler Moffitt, security analyst and resident crypto expert, offers additional insights into the decline in cryptojacking.

He explains, "The trouble with cryptojacking is that it doesn't work well for the average duration of a normal web visit, and ads far outpace script-mining in terms of profitability. Almost all of the sites targeted are streaming sites, where users spend a lot of time. This significantly lowers the adoption rate of this attack vector with criminals."

Despite the decline, he reminds us: "It's not dead yet. Coinhive did shut down in March at all-time cryptocurrency price lows, but CryptoLoot and CoinImp saw some growth during the bull run of April to June. They even posted on Twitter, bragging about death of Coinhive and touting themselves as the new #1 service."

PREDICTION

"Even though cryptojacking websites are declining, I expect cryptomining payloads to stay strong. It's such an effective, low-risk option for criminals. It can target almost any operating system, and there's no reason for victims to know they're infected. The small amounts of crypto are just taken in the form of power costs to the victim. While it's less profitable than ransomware, it's easy, guaranteed money. I think it's going to be around for a long time."

TYLER MOFFITT, SECURITY ANALYST

PHISHING UPDATES

Perhaps some of the most impressive trends we've seen so far this year have been in phishing. There's been major growth in phishing sites, including a huge spike in early April, when the number of phishing sites Webroot-protected customers were prevented from accessing hit nearly 60,000 in a single day. During the first half of 2019, Webroot detected over 1.5 million unique, distinct phishing websites through our end customers' browsing, in addition to another 3.4 million detected via our proactive crawling and analysis of the internet.

> *In particular, close monitoring and inspection of new domain registrations, as well as changes in hosting allocations, are critical for turning predictions of potential phishing activity into zero-day detection of live threats.*
>
> **– Cathy Yang, Product Manager, Threat Intelligence Partnerships**

Phishing targets are also shifting. Traditionally, phishing attacks have tended to impersonate financial institutions. Now attackers seem to be working to obtain credentials to less critical accounts, such as Amazon or FedEx. According to Grayson Milbourne, security intelligence director at Webroot, this is likely due to a variety of factors. Firstly, hacking a financial account can leave more of a digital trail, and because the institution's anti-fraud measures might flag or decline any fraudulent banking activity, it may simply not be worth the effort. Another reason criminals are targeting less critical accounts has to do with password reuse.

Grayson explains that, if a criminal gets ahold of a person's password to a non-essential account, such as Amazon or eBay, this information alone might not be worth much by itself. But if the person reused that password for another account, and the criminal had done some reconnaissance to determine the person's online habits, they might use that password to infiltrate other accounts. And if one such account were work-related, the exposed password could help the attacker access the victims's employer's network.

Additionally, criminals may simply use the information from the non-essential account they'd breached to devise more convincing phishing lures. For instance, if they mimicked an Amazon email and included details about a legitimate order you'd placed, you'd be more likely to take the bait.

> *Today's phishing attacks aren't just going after usernames and passwords. They're also targeting things that might be answers to 'secret questions', such as the name of your first pet or the street you grew up on. Answers to these questions, in combination with info collected from data breaches, can make identity theft much easier to pull off.*
>
> **– Grayson Milbourne, Security Intelligence Director**

SO FAR IN 2019, WE'VE DISCOVERED OVER 1.5 MILLION UNIQUE PHISHING URLS, AND HAVE PROTECTED 3.35 MILLION ENDPOINT DEVICES AGAINST THEM.

THREAT SPOTLIGHT:

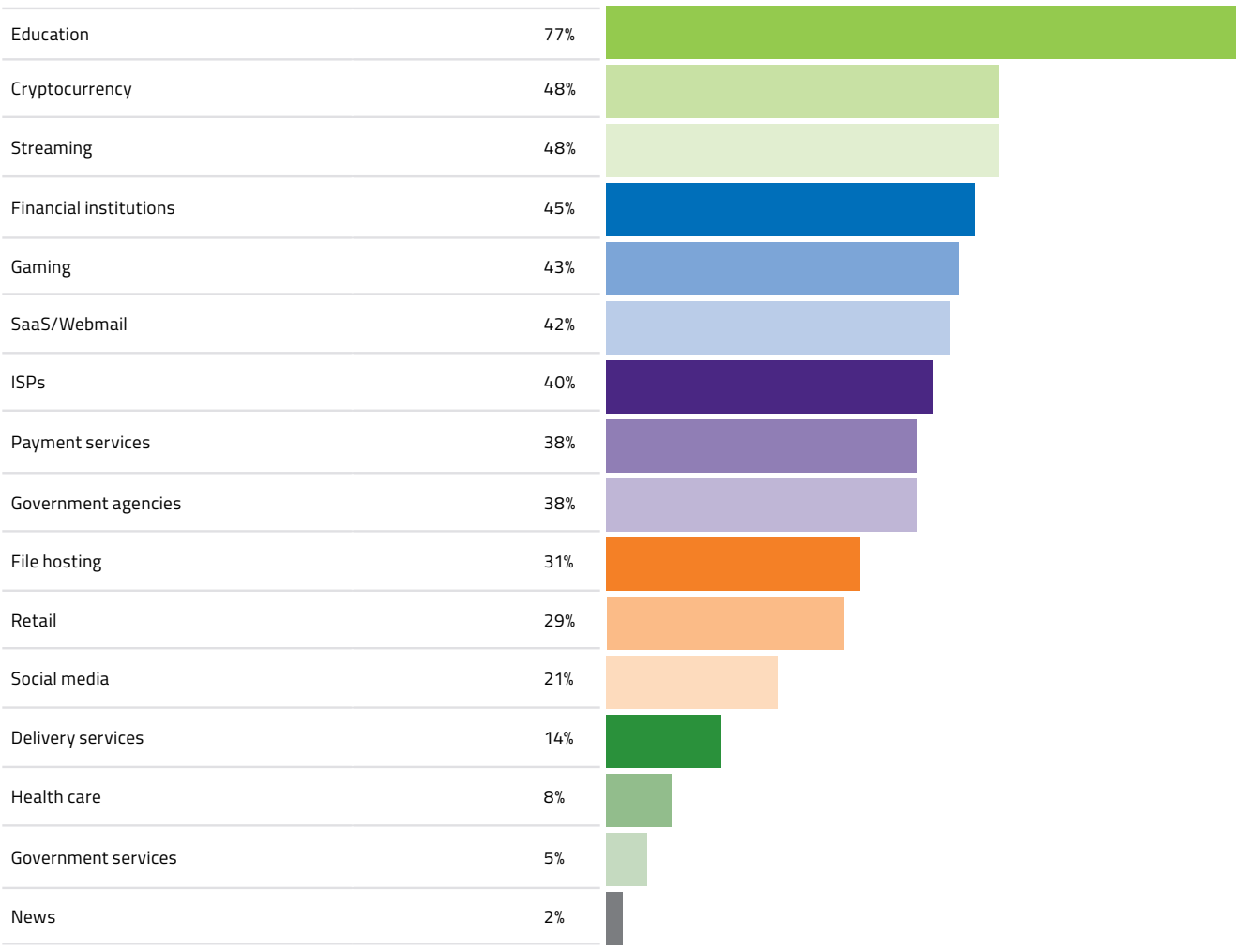
THE HTTPS CONUNDRUM

Nearly 1 in 3 phishing sites use HTTPS.

The HTTPS protocol is giving us a false sense of security, says Hal Lonas, chief technology officer at Webroot. Although the "S" stands for secure, the issue is that HTTPS isn't actually about security. It's about privacy. Hal explains, "when you see that little lock icon in your browser, it just means that the information you transmit on that site is encrypted and securely delivered to where it's going. There's no guarantee that the destination is safe."

According to Hal, because we've all been trained to look for that icon, malicious actors are using HTTPS more and more to create a sense of legitimacy for their bad websites. It's no longer especially difficult to obtain a security certificate, and by doing so, criminals can easily take advantage of users' trust. In fact, nearly 1 in 3 (29%) of all phishing sites we've detected use HTTPS.

PERCENTAGE OF PHISHING WEBSITES (BY CATEGORY) THAT USE HTTPS



If you unwittingly end up on a well-faked phishing copy of your banking website and see the lock icon, it's natural to assume that you're in the right place and all is well. Except when you try to log in, what you're really doing is securely transmitting your login credentials to an attacker. In this case, HTTPS would've been used to trick you.

– Hal Lonas, Chief Technology Officer

PREDICTION

I expect phishing kits will continue to advance, adding further techniques to avoid automatic detection methods. The delivery of phishing pages will also likely become more dynamic, using various conditions to serve a more targeted phishing page which would increase the campaign's likelihood of success.

DAN PARA, SR. THREAT RESEARCH ANALYST

CONCLUSION AND KEY TAKEAWAYS

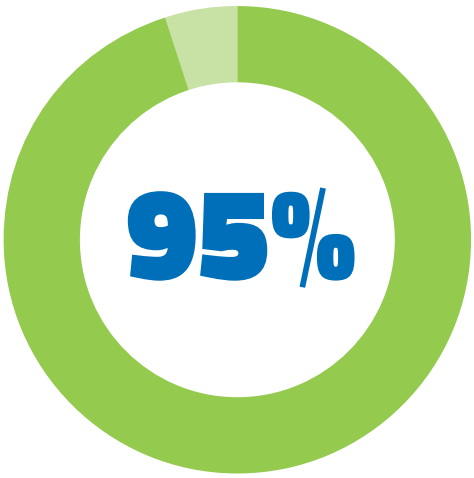
CONCLUSION

The data in this mid-year update to our annual threat report details the trends and changes seen by the Webroot Threat Research Team and within the Webroot Platform, as experienced by our millions of customers worldwide. The first half of 2019 shows how malware authors have continued to evolve their techniques and shift targets.

As cybercriminal tactics continue to evolve, it's clear that predictive protection that can proactively prevent threats before they happen is crucial. Additionally, when end users are educated to avoid phishing and other risks online, they are better prepared to be a strong first line of defense. The continued evolution in phishing indicates the only way for businesses to protect themselves and their customers is by combining predictive security products with relevant, ongoing cybersecurity awareness training.

KEY TAKEAWAYS

Although malware stats remained relatively flat, **nearly all (95%) of the malware we've detected so far was unique to a single PC,** underscoring the need for behavioral protection that can stop polymorphic threats.



MALWARE TARGETING WINDOWS® 7 SYSTEMS HAS RISEN

71%

The number of infections targeting Windows 7 PCs has jumped up significantly, indicating that **malicious actors are specifically targeting older operating systems in hopes of exploiting unpatched vulnerabilities.** (These exploits have led to major attacks in the past, such as when WannaCry used the NSA exploit EternalBlue in 2017.)

As criminals continue to take advantage of operating system vulnerabilities, they're also moving to take advantage of human vulnerabilities, i.e. our trust.

Nearly 1 in 4 malicious URLs (24%) are hosted on trusted domains, banking on site visitors' trust in familiar brands and websites.

Nearly 1 in 3 phishing sites detected (29%) use HTTPS, hoping to trick internet users who are accustomed to looking for and trusting sites that use the "secure" protocol.

About the Data

The Mid-year Update is an extension of the annual Webroot Threat Report, which examines emerging threats and cybercrime trends from the previous year, and shares perspectives and predictions for the future. To read the annual Webroot Threat Report, visit webroot.com/2019ThreatReport

The statistics presented in this annual threat report are derived from metrics automatically captured and analyzed by the Webroot® Platform, our advanced, cloud-based machine learning architecture. This system provides proactive protection for users and networks against both known and zero-day, never-before-seen and advanced persistent threats. Threat intelligence produced by the platform is used by Webroot® endpoint security products and by technology partners through Webroot BrightCloud® Threat Intelligence Services. Our threat intelligence is based on visibility of the entire IPv4 and in-use IPv6 space, billions of URLs, tens of millions of new and updated mobile apps, and all Webroot-protected endpoints worldwide. Advanced machine learning techniques, real-time scoring with confidence levels, and continuous updates enable Webroot threat intelligence to be highly effective at identifying and stopping even the most sophisticated threats. Webroot takes a unique approach to machine learning, based on massive data processing capacity, a proprietary implementation of the most advanced technology available, and a powerful contextual analysis engine. Contextualization is a "guilt by association" model that links internet objects. Capturing an extensive range of characteristics for each internet object observed (up to 10 million characteristics per object) enables Webroot to determine if the object poses a threat at the precise time of analysis. Our patented approach maps attack and threat behavior across vectors, analyzing the relationships among URLs, IPs, files and mobile apps. For example, if a user runs a mobile app that tries to access the contact list and transfer it to an IP address, the malicious behavior of the app would impact the reputation score of the IP address. This ability to correlate current associations among objects with history on how millions of objects have behaved over time is what makes Webroot threat intelligence predictive in nature.

About Carbonite

Carbonite provides a robust data protection platform for businesses, including backup, disaster recovery, high availability and workload migration technology. The Carbonite dataprotection platform supports businesses on a global scale with secure cloud infrastructure. To learn more, visit www.carbonite.com and follow us on Twitter at @Carbonite.

Carbonite, Inc. serves customers through three brands: Carbonite data protection, Webroot cybersecurity, and MailStore email archiving.

About Airlock

The Airlock brand is backed by Ergon Informatik AG, one of the most established and successful IT service providers in Switzerland. Learn more at www.airlock.com.

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks,Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com