Check Point
SOFTWARE TECHNOLOGIES LTD

5TH GENERATION CYBER ATTACKS ARE HERE AND MOST BUSINESSES ARE BEHIND

A New Model For Assessing and Planning Security

GEN V

TABLE OF CONTENTS

BACKGROUND

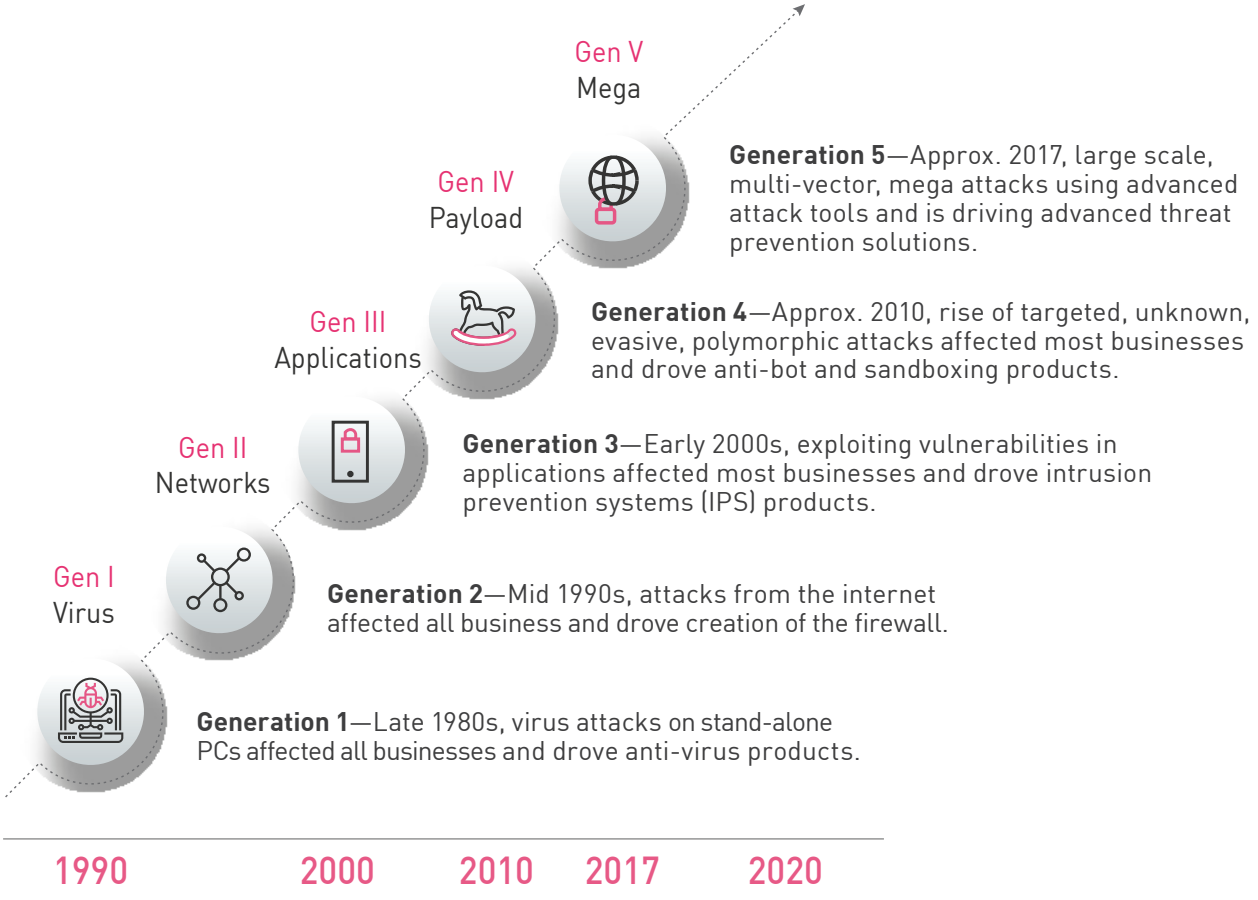
In the last 25 years, attacks and security protection have advanced rapidly. Looking back it is easy to identify the different generations of attacks and security products that protect against them. However, today the velocity of attack evolution is far outpacing the level of security that businesses have deployed. This is a problem. The level of security deployed by businesses cannot lag behind the level of attacks coming at them. Today's attacks are the most advanced and impactful we've ever seen and yet the security deployed by most businesses is generationally outdated and incapable of protecting against these attacks.

There are many reasons security infrastructures have fallen behind as the level of attacks has risen. The most obvious is attackers have no constraints. They can create and push the envelope, even recklessly, in developing new and advanced techniques. Businesses, of course, have change control procedures, budgets, compliance and myriad other operational constraints to which they must adhere, thus restraining security advancement. Another is the traditional check box method of building a security infrastructure whereby a specific security technology is deployed to defend against a specific type of attack or to protect a specific type of application. This binary, mono-vision approach, aka "point solution," was effective in earlier generations when attacks were one-dimensional but today's attacks are multi-everything—multi-dimensional, multi-stage, multi-vector and polymorphic. To properly protect a business's IT operations today requires a new, holistic approach to assessing and designing their security toward an integrated and unified security infrastructure that prevents attacks in real time.

The generational framework described in this paper is a new and very important tool for businesses to realistically assess their current security infrastructure versus the level of attacks that occur daily. This is a brand new and very effective way to assess one's security posture. For most businesses, this assessment will reveal the stark reality that despite their best efforts, their level of protection is generationally behind the level of attacks coming at them.

The Generations of Attacks and Security

It is the appearance and then the continued advancement of attacks that drove the creation and then subsequent advancement of security products. Looking back, one can see clear generational delineations of attack-then-protection advancements, with each generation more sophisticated than the prior. Networking—and then the Internet—connected people, governments and businesses like never before in human history. This connectivity also created a vast new frontier, in fact a new, target-rich hunting ground for malicious actors and illicit activity. From curious hackers to corporate and state sponsored espionage to organized crime, the new networked world provided near unimpeded access to all sorts of assets and private data—with near complete anonymity! As a result, every successful advancement of malicious activity drove corresponding advancements in IT security. This cycle will certainly continue.



"Only 5% of enterprises are using Gen 5 Cyber Security"

GENERATION 1

OVERVIEW

The first generation began in the 1980s and coincided with the mass availability and use of personal computers by the general public. Virus attacks, which are malicious software programs that replicate themselves on new computers, soon emerged. These virus attacks affected all businesses and users of personal computers. The impact of virus attacks was large and disruptive enough that commercial anti-virus software products were developed to protect against them.

Proliferation
Personal computers operated as stand-alone devices. Portable floppy disks were used to share files between users and personal computers—and is also how viruses proliferated.

Attackers
This era is where "hacker in his parent's basement" originated. The term "computer hacking" and ultimately "hacking" became common reference in the 1980s to refer to those who write software programs to disrupt or attack computers. The hackers were mostly inquisitive teenagers hacking for the sheer fun and challenge of breaking into systems. Writing viruses was also done in the pursuit of knowledge and to build a personal reputation as a creator of clever programs. Evolving beyond individuals, the hacker underground advanced and organized through bulletin board systems (BBS) which granted anonymity and freedom to share knowledge and trophies among peers.

Examples of Well known Generation 1 Attacks

Elk Cloner
Elk Cloner is known as the first virus written and released to infect personal computers. Coded by then 15-year old Richard Skrenta as a joke, it served as an annoyance and occasionally displayed a poem on the infected computer.

> *"When Rich Skrenta created Elk Cloner as a prank in February 1982, he was a 15-year-old high school student with a precocious ability in programming and an overwhelming interest in computers. The boot sector virus was written for Apple II systems, the dominant home computers of the time, and infected floppy discs.*
>
> *If an Apple II booted from an infected floppy disk, Elk Cloner became resident in the computer's memory. Uninfected discs inserted into the same computer were given a dose of the malware just as soon as a user keyed in the command catalog for a list of files.*

> *Infected computers would display a short poem, also written by Skrenta, on every fiftieth boot from an infected disk:*
>
> *Elk Cloner: The program with a personality*
>
> *It will get on all your disks It will infiltrate your chips Yes it's Cloner!*
>
> *It will stick to you like glue It will modify ram too Send in the Cloner!"* [1]

Brain

Brain is known as the first worldwide virus. It was created in 1988 by mistake when two brothers, Basit and Amjad Farooq Alvi wrote what they thought was a mechanism to halt illegal copying of their software products. However, their design was flawed and their tool became an actual virus that copied and replicated itself.

> *"The first worldwide PC virus, Brain worked by changing the boot sector of a floppy. When an infected floppy was put into a computer, it installed Brain in the computer's memory, from where it infected new floppies as they were inserted."* [2]

Security Technologies Developed as a Result of Generation 1 Attacks

In response to the growing number of viruses and disruptive software, many tools and eventually commercial products were developed to combat them, specifically anti-virus products. Two early examples are:

- In 1985 G Data Software released their first anti-virus product for the Atari ST platform. [3]
- In 1987 John McAfee founded McAfee and released their first anti-virus product VirusScan.

> *Prescient and foretelling, in 1987 Fred Cohen wrote "... there is no algorithm that can perfectly detect all possible computer viruses."* [4]

Security Infrastructure Implications

While there were password controls to access PCs and possibly further controls to access files on individual PCs, the only "IT infrastructure" of this generation was anti-virus products.

---

1. Reference: *https://www.theregister.co.uk/2012/12/14/first_virus_elk_cloner_creator_interviewed/*
2. Reference: http://www.zdnet.com/pictures/ten-computer-viruses-that-changed-the-world/
3. Reference: *https://en.wikipedia.org/wiki/Antivirus_software*
4. Reference: *https://antivirussw.weebly.com/history.html*

GENERATION 2

OVERVIEW

The second generation emerged in the 1990s with the advent of networking and the internet. Everyone was "going online." With networks connecting computers and the internet connecting governments, businesses and the public, the gates were opened for the broad and rapid spread of malicious and volatile software. This unencumbered access to anything and everything connected, led to the development of the network firewall.

Proliferation
Network connectivity advanced information sharing from the speed of hand carrying floppy drives to computer speed over connected networks—and the speed and spread of attacks grew equally.

Attackers
The advent of networking brought an end to hacker BBSs as hackers moved to organize and communicate through the World Wide Web (WWW) and websites. The increased connectivity increased the spread and damage of curious pranksters and also began the earliest, fledgling stages of cybercrime and theft.

Examples of Some Well known Generation 2 Attacks

Morris Worm
The Morris worm was launched in the very early days of the Internet, on November 1988. Robert Morris, a graduate student at Cornell University, created the Morris Worm with innocent intentions. He claims he wrote the worm in an effort to gauge the size of the Internet. Unfortunately, the worm contained an error that caused it to repeatedly infect computers which consumed resources creating a denial of service conditions. The Morris Worm is said to have infected as many as 60,000 host systems across the young Internet and served notice that network and Internet security was severely needed.

> *"The source code also shows that Morris attempted to keep the spread of the worm under control, but he was more confident in his code than he should have been. Bugs in the code caused it to crash many systems, basically all SunOS systems, and to execute more than once on many other systems, devouring system resources."* [5]
>
> *"Everyone realized at the time that computer security was no longer just theory, but something that needed to be taken seriously."* [6]

5. Reference: http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/
6. Reference: http://www.zdnet.com/article/the-morris-worm-internet-malware-turns-25/

First Cyber Theft?

The article "*The First Great Cyber Crime: 1994 Attack Against Citibank*" on CTOVision.com anoints this attack as possibly the first monetary theft by cyber attack. It is described by the U.S. FBI:

> *"The global dimensions of cyber crime, though, became apparent as early as 1994. That summer, from deep inside the heart of Russia, a young computer wiz named Vladimir Levin robbed a bank in the U.S. without ever leaving his chair. Over a two-month period, Levin—with the help of several conspirators—hacked into Citibank computers and transferred more than $10 million to accounts around the world using a dial-up wire transfer service. Working with Citibank and Russian authorities, FBI agents helped trace the theft back to Levin in St. Petersburg. Levin was soon lured to London and arrested."*

Melissa Virus

In 1999, David Smith, a network programmer, released the Melissa Virus to the Internet. It was contained in a Microsoft Word document macro that when opened would email itself to the first 50 addresses in the MAPI email address file on the computer. Smith's motivation was apparently curiosity. Melissa crashed 100,000 email servers and caused $80M in damages.

> *"'Melissa.A' used social engineering techniques, since it came with the message, "Here is the document you asked me for...do not show it to anyone." In just a few days, she starred in one of the most important cases of massive infection in history, causing damage of more than 80 million dollars to American companies. Companies like Microsoft, Intel and Lucent Technologies had to block their Internet connections due to its action."*[7]

Security Technologies Developed as a Result of Generation 2 Attacks

In response to the "Wild West" of free and open access to all things networked, security innovators and entrepreneurs developed the network firewall to control access to private networks from the public internet. In its most basic sense, the network firewall is a barrier between two networks through which all traffic must flow and the firewall has rules to determine which traffic is allowed while the other traffic is blocked. Examples of the earliest firewalls are:

Digital Equipment Corporation released the DEC SEAL firewall product in 1991.

7. Reference: https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/

In 1994 the open source Firewall Toolkit (FWTK) was released as the Gauntlet Firewall by Trusted Information Systems.

Also in 1994, Check Point introduced Firewall-1, the first "stateful inspection" firewall in which the product tracks operating state and assesses each packet within the context of its open connection.

Security Infrastructure Implications

Firewall and anti-virus products are essential to protect any business or other entity that is connecting their internal networks to the internet. The claim can be made that firewall and anti-virus are the first true IT "security infrastructure." This era also marks the beginning of the "point solution" security model to select and deploy ad hoc products to protect against specific threats or to protect specific services.

GENERATION 3

OVERVIEW

The third generation emerged in the early 2000s as attackers learned to leverage vulnerabilities in all components of an IT infrastructure. IETF RFC 2828 defines "**vulnerability**" as *"A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy."*

And vulnerabilities were plentiful. At any given time, multiples of them existed in operating systems, applications—any element of an IT infrastructure had vulnerabilities that an adept attacker could take advantage of to gain access to a private network. Attacks targeting vulnerabilities could not be effectively stopped by firewalls, anti-virus or intrusion detection system (IDS) products. So, IDS products advanced into intrusion prevention systems (IPS) to not only detect but to actually prevent attacks targeting vulnerabilities.

Proliferation

"Sophistication" is an oft-used word to describe cyber-attacks and this generation showed the first hints of attack sophistication. Instead of writing a virus or worm that spreads erroneously, by happenstance, in this era attackers began to analyze networks and software products to specifically identify weaknesses and vulnerabilities to which they could design attacks to penetrate and disrupt operations and/or steal assets. And sometimes their attack was wrapped in a warm blanket of "social engineering" that enticed users to "click" and initiate the infection.

Attackers

The IT industry is booming, creating new products, tools, applications and services to meet the needs of a hungry market that is actively and aggressively moving everything online—and attackers are learning of the bounty that awaits them. They become more organized and sophisticated and are less interested in notoriety and more interested in making money through illicit means, cyber hacking.

Examples of Some Well known Generation 3 Attacks

ILOVEYOU

The ILOVEYOU virus launched on May 4, 2000 and in a matter of minutes infected thousands of computers. It was so far reaching and impactful that it made the cover of *Time* magazine in May 2000. Companies and anti-virus vendors screened emails with a title of "ILOVEYOU" but attackers simply changed the title to continue its proliferation.

> *"The ILOVEYOU virus comes in an e-mail note with "I LOVE YOU" in the subject line and contains an attachment that, when opened, results in the message being re-sent to everyone in the recipient's Microsoft Outlook address book and, perhaps more seriously, the loss of every JPEG, MP3, and certain other files on the recipient's hard disk. Because Microsoft Outlook is widely installed as the e-mail handler in corporate networks, the ILOVEYOU virus can spread rapidly from user to user within a corporation. On May 4, 2000, the virus spread so quickly that e-mail had to be shut down in a number of major enterprises such as the Ford Motor Company. The virus reached an estimated 45 million users in a single day."* [8]

SQLSlammer

SQLSlammer, aka Sapphire among other names, attacked vulnerabilities in Microsoft SQL Server and MSDE and became the fastest spreading worm of all time.

> *"As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes." ... The worm "began to infect hosts slightly before 05:30 UTC on Saturday, January 25. Sapphire exploited a buffer overflow vulnerability in computers on the Internet running Microsoft's SQL Server or MSDE 2000 (Microsoft SQL Server Desktop Engine). This weakness in an underlying indexing service was discovered in July 2002; Microsoft released a patch for the vulnerability before it was announced. The worm infected at least 75,000 hosts, perhaps considerably more, and caused network outages and such unforeseen consequences as canceled airline flights, interference with elections, and ATM failures."* [9]

8. Reference: http://searchsecurity.techtarget.com/definition/ILOVEYOU-virus
9. Reference: https://www.caida.org/publications/papers/2003/sapphire/sapphire.html

Estonia

On April 27, 2007, European Union and NATO member country Estonia fell under massive cyber-attacks against its infrastructure.

> These attacks *"... swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn. Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred."* [10]

Security Technologies Developed as a Result of Generation 3 Attacks

The very young but very vibrant and entrepreneurial security industry responded to the explosion of vulnerabilities and vulnerability attacks with Intrusion Detection System (IDS) products which soon evolved to Intrusion Prevention System (IPS) products. After all, if you can detect an attack, then why not prevent it? The primary protection provided by IPS products is to protect known vulnerabilities from being exploited. These are signature-based products, meaning a signature is written for as many known, high profile vulnerabilities as possible to detect activity that appears to be taking advantage of a vulnerability. IPS products are truly an advancement beyond the firewall and anti-virus because IPS products inspect the network traffic, packet by packet, looking for signature matches or anomalous, suspicious activity. When a match is made, the attack is blocked. However, accuracy in prevention is a challenge and "false positives" are a hindrance to wide adoption of IPS.

Security Infrastructure Implications

This era saw an explosion of technologies and services and in turn a greater explosion of security vendors and products to secure them. Security startups and security vendors were building new products, each specializing in different "slices" of security, from firewall to anti-virus to intrusion detection to web application to peer-to-peer to internet telephone, and many, many more.

This is also the era where the "point solution" model for building security infrastructures began to get heavy. For each new type of attack and each new type of IT service and application, businesses would often add a new security product to protect against that attack or to protect that service. In nearly all cases, the new product would be from a different security vendor who specialized in the area of security needed. A security infrastructure comprised of multiple different products from multiple different vendors, each with their own user interface and physical management station, began to get heavy and operationally inefficient. Most importantly, the level of protection began falling behind the level of attacks being launched.

10.Reference: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

GENERATION 4

OVERVIEW

The fourth generation emerged in approximately 2010 as attackers reached new levels of sophistication. In fact, attackers and their methods became professional. The attacks ranged from international espionage to massive breaches of personal information to large scale internet disruption. This generation's attacks made headlines in daily, mainstream media simply because of the large scale impact on and relevance to the general public. The attacks impacted board rooms, CEOs and caused governmental investigations.

While internet security of the 2nd and 3rd generations provided access control and inspected all traffic, it was severely lacking in validating the actual end-user content received in email, through file downloads and more. Attacks were hidden in everything from resumes to picture files and behind them awaited sophisticated code ready to launch and spread and sometimes was further supported by massive bot armies ready to storm the gates. All that was needed was for a user to do their job—such as opening an attachment in the official looking email in their In-box or download a business file from the internet or plug a USB into their laptop—and the attack was silently launched. The attack could search for customer databases and exfiltrate personal information, or via communication back to "Command&Control" (C&C) initiate a massive bot-driven denial of service attack for purposes of disruption or as a decoy for the real attack, and much more.

Proliferation

Sophistication increased dramatically in this generation—and is a firm indication of things to come. The headline breaches were a result of attacks that were specifically designed and "engineered" to compromise the target and exfiltrate information to sell on black markets and/or to cause major disruptions. The proliferation was different and more dangerous than prior generations as unintentional leakage of the sophisticated attack tools beyond the original target educated the general hacker world and so increased the overall attacker sophistication more than what it otherwise would have been. For example, the Stuxnet worm spread beyond its original target as elements of it were later found in other attacks and today can be downloaded by anyone.

Attackers
In this generation the generic "attackers" evolve into a more organized and more formidable force. They become truly professional organized crime entities and nation states leverage their own cyber forces essentially as an arm of their military—all for the purposes of manufacturing cyber-attacks for money or disruption or both.

Examples of Some Well known Generation 4 Attacks

Discovered in the Fall of 2010, the Stuxnet worm attacked Iran's Natanz nuclear refinement facility. Described by some as the most advanced attack ever designed, Stuxnet searched for the specific Siemen's controllers that managed the nuclear centrifuges in Iran's facility and once infected, stealthily caused them to spin out of control, ultimately causing physical damage to the centrifuge equipment.

> *"But in 2010, Stuxnet escaped Natanz, probably on someone's laptop; once connected to the outside Internet, it did what it was designed not to do: spread in public."* [11]

It was later reported that Stuxnet was created via a joint effort between the United States and Israel in an effort to impede Iran's nuclear ambitions.

Target
In December 2013, Target, the third largest US retailer reached headlines over a cyber-attack that planted malware on their point of sale (POS) system and compromised upwards of 40 million customer credit and debit cards and the private information of as many as 110 million customers (various reports claim from 70 to 110 million). It was reported that the attackers first breached the network of Target's HVAC provider who had remote access to Target's network for purposes of HVAC service in some Target stores. From there the attackers were able to plant the malware in the Target point of sale (POS) system to capture and export credit card and other personal information before it was encrypted and sent on to Target's transaction processing. The financial impacts of the breach were estimated to reach into hundreds of millions of dollars with some estimates as high as $1B [12]. In addition,Target's CEO and Board Chairman Gregg Steinhafel resigned. [13]

As indicator of this generation of attacks, here are three very revealing points about this attack and breach:

- The HVAC company's access should have been segmented from the rest of the business network. This is also required to comply with the Payment Card Industry (PCI) standard for businesses who conduct credit card transactions. [14]

11. Reference: *https://www.forbes.com/sites/christopherskroupa/2017/04/19/the-cost-of-cyber-breach-how-much-your-company-should-budget/#1a4c8926ce74*
12. Reference: https://www.forbes.com/sites/christopherskroupa/2017/04/19/the-cost-of-cyber-breach-how-much-your-company-should-budget/#1a4c8926ce74
13. Reference: *http://www.zdnet.com/article/target-ceo-out-after-massive-cyberattack-cfo-to-replace/*
14. Reference: *https://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html*

- There are reports that one of Target's point solution products actually detected the attack but because it was "detect-only," did not block it and amidst many detection alerts, the Target team initially missed the attack.

> *" 53.7 million—The income that hackers likely generated from the sale of 2 million cards stolen from Target and sold at the mid-range price of $26.85 (the median price between $18.00 and $35.70)."* [15]

DYN

On Friday, October 21, 2016, cyber security reached yet a new level of public awareness, as the world learned that an army of bots hosted on internet connected cameras were able to cause outages to well known internet services such as Twitter, Amazon, Spotify and Netflix. The global Distributed Denial of Service (DDoS) attack on DYN, a large DNS infrastructure company, caused the downtime. It may not have shocked internet security professionals, but it gave yet another demonstration of the fragility of the Internet grid. Fortunately, it was not as damaging as it could have been. [16]

> *"During a DDoS that uses the DNS protocol, it can be difficult to distinguish legitimate traffic from attack traffic. For example, the impact of the attack generated a storm of legitimate retry activity as recursive servers attempted to refresh their caches, creating 10-20X normal traffic volume across a large number of IP addresses. When DNS traffic congestion occurs, legitimate retries can further contribute to traffic volume. We saw both attack and legitimate traffic coming from millions of IPs across all geographies. It appears the malicious attacks were sourced from at least one botnet, with the retry storm providing a false indicator of a significantly larger set of endpoints than we now know it to be. We are still working on analyzing the data but the estimate at the time of this report is up to 100,000 malicious endpoints. We are able to confirm that a significant volume of attack traffic originated from Mirai-based botnets."* [17]

Security Technologies Developed as a Result of Generation 4 Attacks

This generation very clearly marked the point where "signature only" security was not enough. These products detect attacks based on "signatures" that are created AFTER an attack is discovered, analyzed and communicated to the market. The window of exposure for businesses is days and can even be months until a "patch" is written to fix the vulnerability. So with more sophisticated malware that is "new" (so no signatures to detect it) and far advanced beyond the signature-based security of the day, new technologies to defend against "previously unknown" and "zero-day attacks" were developed. Specifically, technologies to protect against attacks from bot networks and to inspect all files ingress before user access were created. These are commonly known as "anti-bot" and "sandbox" technologies. And with their emergence some businesses added two more "point solution" products to their environment, further complicating their non-integrated security infrastructure.

15. Reference: *https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*
16. Reference: *http://blog.checkpoint.com/2016/11/08/denied-dealing-global-distributed-denial-service/*
17. Reference: *https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/*

GENERATION 5

OVERVIEW

The 5th generation emerged in approximately 2017 as leakage of advanced tools drove large scale, multi-vector, mega attacks that generated revenues and disruption for the criminals and caused major impacts on a large scale. This led to custom, sophisticated malware that can infiltrate and proliferate from and to virtually any vector of an IT infrastructure—including a business's networks, cloud instances, remote offices, mobile devices, third parties and more. This latest, 5th generation of attacks is well described in ***The Global Risks Report 2018, 13th Edition***, "*... incidents that would once have been considered extraordinary are becoming more and more commonplace*." And the report later cites two attack examples during 2017 saying, "*...the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses of US$300 million for a number of affected businesses*."

Proliferation

The 5th-generation attacks move very fast and in mere hours infect large numbers of businesses and entities across large geographic regions. Yes, the viruses of earlier generations also moved fast but these 5th-generation attacks are fast and highly sophisticated, stealthy—and successful. For example, the WannaCry attack leveraged a tool called EternalBlue that was developed by the United States National Security Agency—and was presumably unintentionally leaked to the cyber world. The tool exploited vulnerabilities in Microsoft Windows XP to many different attacker whims from ransomware to pure disruption. 5th generation attacks are an escalated threat over prior generations because they are multi-vector and mega because they can infiltrate and quickly and silently proliferate from and to any vector of an IT infrastructure including networks, cloud instances, remote offices, endpoints, mobile devices, 3rd parties and more.

Attackers

If you are still unsure about the seriousness and capabilities of 5th-generation cyber criminals, consider these points from https://www.knowbe4.com/resources/five-generations-of-cybercrime/

- Cybercrime has its own social networks with escrow services
- Malware can now be licensed and gets tech support
- You can rent botnets by the hour, for your own crime spree
- Pay-for-play malware infection services that quickly create botnets
- A lively market for zero-day exploits (unknown vulnerabilities)

Clearly as of this writing in Q1 2018, cyber criminals are very organized, even industrialized as any business honed for success would be. The attackers are technically savvy and as new technologies emerge in the marketplace, they will quickly exploit it for their purposes and to the detriment of their target.

Examples of Some Well known Generation 5 Attacks

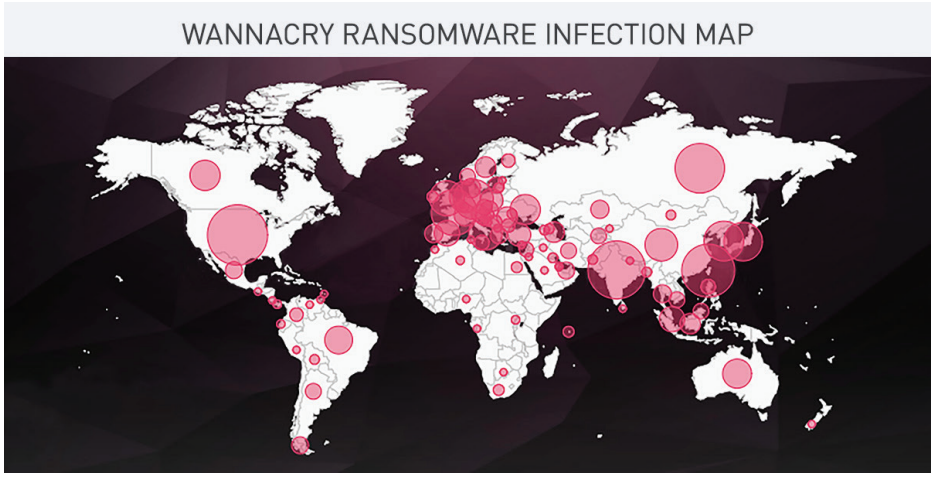
WannaCry

In May 2017 the WannaCry ransomware attack hit and targeted computers running the Microsoft Windows XP operating system worldwide. The attack encrypted data and then demanded a ransom payment to be made in Bitcoin. WannaCry leveraged a tool called EternalBlue that was developed by the United States National Security Agency—and was presumably unintentionally leaked to the cyber world.

Ironically, the patch needed to prevent WannaCry infections was actually available before the attack began: Microsoft Security Bulletin MS17-010, released on March 14, 2017, updated the Windows implementation of the SMB protocol to prevent infection via EternalBlue. However, despite the fact that Microsoft had flagged the patch as critical, many systems were still unpatched as of May of 2017 when WannaCry began its rapid spread.[18]

A number of factors made the initial spread of WannaCry particularly noteworthy: it struck a number of important and high-profile systems, including many in Britain's National Health Service; it exploited a Windows vulnerability that was suspected to have been first discovered by the United States National Security Agency; and it was tentatively linked by Symantec and other security researchers to the Lazarus Group, a cybercrime organization that may be connected to the North Korean government.[19]

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. [20]



As of May 17, 2017, Source: Check Point Software Technologies Blog, http://blog.checkpoint.com/2017/05/17/check-point-reveals-global-wannacry-ransomware-infection-map-cpx-europe-2017/

18. Reference: *https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html*
19. Reference: *https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html*
20. Reference: *https://en.wikipedia.org/wiki/WannaCry_ransomware_attack*

NotPetya

In March 2016 Petya ransomware appeared. It encrypted hard drives and demanded a ransom in exchange for the key to decrypt the files. Then in June 2017 an attack initially thought to also be Petya attacked banks, airports and power companies in Ukraine, Russia and parts of Europe. After deeper analysis it was dubbed NotPetya because it truly was not ...

> *The original Petya required the victim to download it from a spam email, launch it, and give it admin permissions. NotPetya exploits several different methods to spread without human intervention. The original infection vector appears to be via a backdoor planted in M.E.Doc, an accounting software package that's used by almost every company in the Ukraine. Having infected computers from Medoc's servers, NotPetya used a variety of techniques to spread to other computers, including EternalBlue and EternalRomance, two exploits developed by the United States NSA to take advantage a flaw in the Windows implementation of the SMB protocol. It can also take advantage of a tool called Mimi Katz to find network administration credentials in the infected machine's memory, and then use the PsExec and WMIC tools built into Windows to remotely access other computers on the local network and infect them as well.* [21]

The Petya attack encrypted files and actually offered a process to pay ransom to attain the decryption key to free the files. NotPetya also encrypts files but only appears to offer a means to buy the decryption key. The token on its ransom screen is merely a randomly generated number that is meaningless.

> *So what's NotPetya's real purpose? The fact that it saw an abrupt and radical improvement in efficiency over its Petya ancestor implies a creator with a lot of resources—a state intelligence or cyberwarfare agency, say. That, combined with the 2017 attack's focus on the Ukraine, caused many to point their finger at Russia, with whom Ukraine has been involved in a low-level conflict since the occupation of Crimea in 2014. This accusation was taken up by the Ukrainian government itself, and many Western sources agree, including the U.S. and U.K.; Russia has denied involvement, pointing out that NotPetya infected many Russian computers as well.* [22]

However, among the most impacted by the attack is one of the largest shipping companies in the world, A.P. Moller-Maersk. Based in Copenhagen, the attack caused shipping delays and disruption for weeks and an estimated financial impact of between $200-$300 million. [23]

21. Reference: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
22. Reference: https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
23. Reference: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#16ab49f84f9a

Security Technologies Developed as a Result of Generation 5 Attacks

The 5th generation of attacks are highlighting the need for integrated and unified security infrastructures, in fact security "architectures." Attack vectors and proliferation paths include anything that is internet connected, whether on premises, remote or mobile, or with shared connections to third parties. As we've learned, the 5th generation attacks are designed for target success, move very fast across any element of an IT infrastructure and operate with incredible stealth. The prior generations of security are non-integrated, point solution, detect-first technologies that are overmatched and cannot protect against the new "formerly extraordinary and now commonplace" attacks of the 5th generation.

For example, sandboxes from 4th generation allow the first attack to infect a "patient zero" and thus the network while the sandbox analyzes and builds indicators to detect reoccurrences of the same attack. This is not good enough and is clearly behind the capabilities of 5th-generation attacks. 5th-generation attacks like WannaCry and NotPetya, combined with the new dynamic IT services enabled by mobile access and on-demand, elastic cloud computing service, require a brand new model for assessing and building security infrastructures. This is the 5th generation model for IT security and is an integrated and unified security architecture that shares threat intelligence in real time for fast, real time, inline prevention on the first occurrence of an attack.

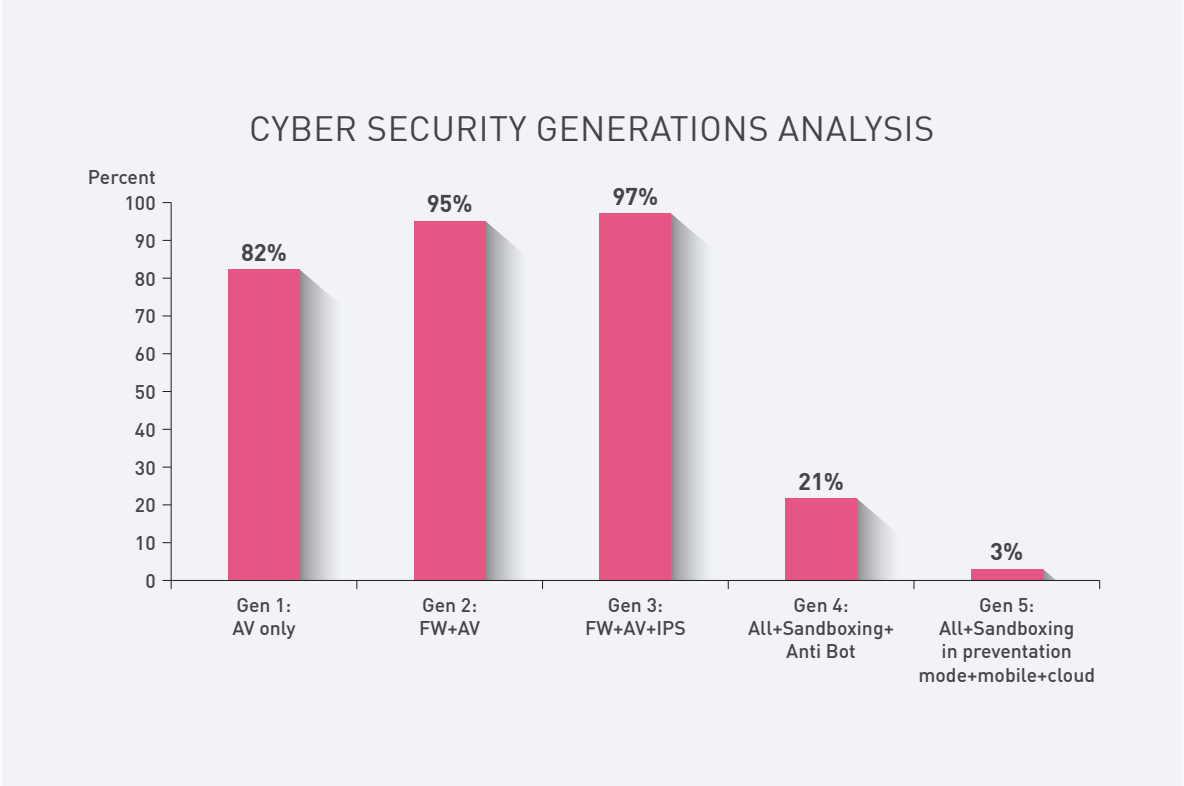
> **5th-generation attacks are designed for target success, move very fast, and operate with incredible stealth.**

INSIGHTS

Assessing and viewing security from this generational view gives a new and very revealing perspective. In fact this new model and new perspective is much needed in IT security because the old, traditional methods are failing. Viewing and assessing IT security through the generational lens reveals some very urgent and even startling insights.

1. Business security levels are behind the level of attacks coming at them.

Specifically, most businesses are only at the 2nd and 3rd generation of security and yet as we've just read, today's attacks are in the far more advanced and damaging 5th generation. In Q1 2018, Check Point surveyed 443 security professionals around the world about their security infrastructures and the results validate that most security infrastructures are generationally and dangerously behind the level of attacks they must protect against. This state of affairs is indeed urgent and startling.

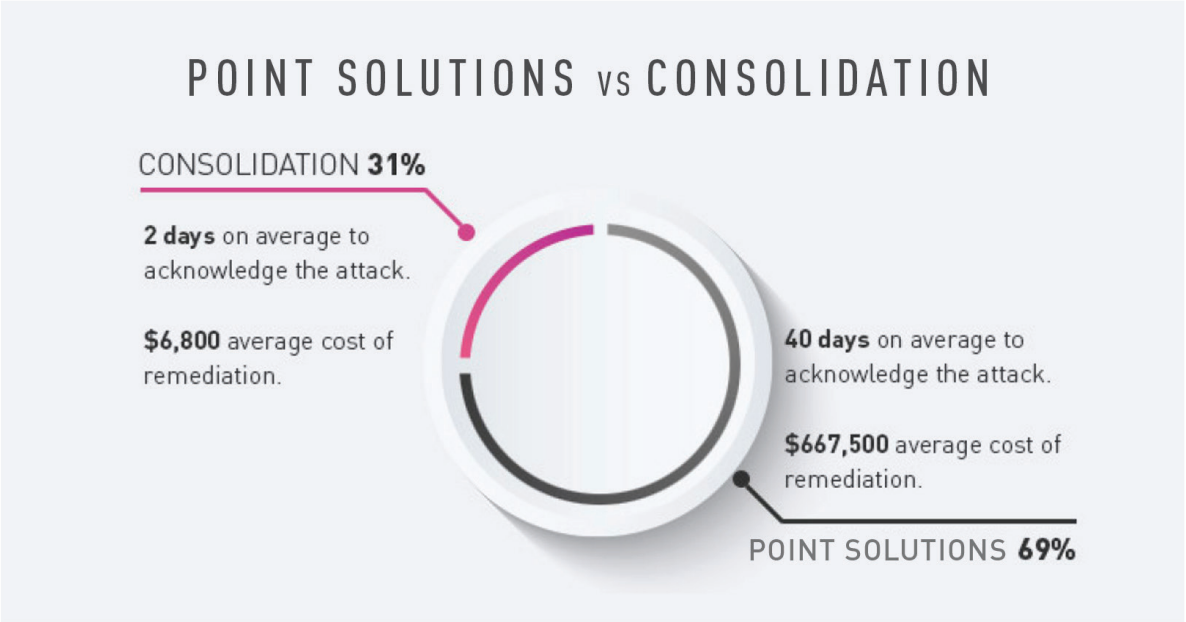


Why and how can this happen? The velocity of attack advancement is much faster than business's ability to assess, select and deploy new security technologies required to protect against the new attacks. Attackers operate freely and can advance without hindrance while businesses are inhibited by up-time requirements, change control, compliance controls, staffing shortages, budget restrictions—and their point solution security infrastructure. It is difficult to continue adding more products to an already operationally heavy security infrastructure. The bottom line is that businesses cannot keep up.

2. A new model is needed for assessing threats and security.

In the early generations it was effective to add a new security product for every new type of attack or application. However, "there's a new attack—deploy a new security product" model of designing and deploying security does not work. This approach produces a security infrastructure of "point solution," non-integrated products without central threat sharing or management. And because they are not integrated and cannot share real time attack information, the most timely and best accuracy is sacrificed and thus most are "detect-only." These point solution deployments are inefficient operationally because they can be comprised of 20-30 and more security products. Managing so many products requires more security staff—at a time when there is a shortage of security expertise. So in spite of business's best efforts, typical IT security infrastructures of today are "generationally behind" and incapable of protecting against the attacks being launched.

As evidence to this point, in a recent survey executives were asked various questions about their cyber security requirements, including their day-to-day challenges and concerns. One of the questions asked was what do they consider the best approach. Overwhelmingly, C-level executives stated they were satisfied with a point solution strategy and promoted it within their organization. However, once asked more probing questions regarding their security posture, it became obvious that their sense of what was best for their organization was a false sense of security, noting a significant difference in the attack recovery processes:



As evidenced by the survey result above, using the generational model to assess threats and their current security infrastructure will drive a much different and very valuable, new perspective. It will also drive better security with more efficient operations at a lower cost.

3. 5th Generation security is required.

As we've seen, most businesses are only at the 2nd and 3rd generation of security while today's attacks are 5th generation—and cyber criminals and cyber-attacks are only going to continue to advance in organization, sophistication and speed. Businesses need to build a plan to move from their point solution security deployment to a 5th-generation security infrastructure. 5th-generation security is advanced threat prevention that uniformly prevents attacks on a business's entire IT infrastructure of networks, virtual instances, cloud deployments, endpoints, remote offices and mobile devices with a single, central management for administration, monitoring and response. It is a foundation that not only protects against 5th-generation attacks but is also an architecture upon which businesses can easily and efficiently add security capabilities as threats advance and IT environments evolve.

What Is 5th Generation Security?

5th-generation security is marked by the following advancements over the prior 4th-generation security:

- **Consolidates** prior generation security of next-generation-firewall (NGFW), sandbox, bot security, endpoint security and other security controls into a single unified security system.
- **Shares** real time threat information in real time throughout the system.
- **Prevents** advanced 5th-generation and first occurrence of new attacks; does not allow first-attack "patient-zero" infection.
- **Extends** prevention of advanced attacks to cloud deployments and mobile devices as part of the single, unified security system.
- **Uniformly** prevents attacks across a business's entire IT infrastructure of computer networks, virtual instances, cloud deployments, endpoints, remote offices and mobile devices.
- **Centrally** manages, monitors and responds to all security activities and events as a single, unified security system.

This is 5th-generation security and this is Check Point Infinity. Check Point Infinity is the only fully consolidated cyber security architecture that protects your business and IT infrastructure against Gen V mega cyberattacks across all networks, endpoint, cloud and mobile.

The architecture is designed to resolve the complexities of growing connectivity and inefficient security. It provides real-time threat prevention against known and unknown threats, leveraging the most advanced threat prevention and zero-day technologies. Additionally, automatic threat intelligence sharing across all networks, endpoint, cloud and mobile, delivers consistent security across all Check Point components and seals security gaps.

Check Point Infinity architecture consolidates management of multiple security layers, providing superior policy efficiency and the ability to manage security through a single pane of glass. The single management centrally correlates all types of events across all network environments, cloud services and mobile infrastructures.

SUMMARY

The advancement and societal benefits brought by computing technology is truly stunning. When I graduated high school in 1980, I had never even touched a "computer." I earned my college degree primarily on an IBM Virtual Machine (VM) mainframe environment and some of my first class projects were developed on punch cards. Today I can communicate with family, friends and business associates and access my business networks and untold information and assets from practically anywhere in the world with an amazingly small, hand held smart phone. The advancement is truly remarkable. And yet if I as an individual resist joining the technology world, or just allow myself to fall behind, I am at a societal disadvantage because I am less connected and without the wealth of information and efficiency that smart phones and computing provide to me individually.

The evolution of cyber-attacks and cyber security is equally stunning. What began in the early 1980s for curiosity, fun and notoriety is today a multi-billion dollar industry for organized crime. Equally, essentially born in the 1980s, the IT security industry is a multi-billion dollar industry that is vital, in fact absolutely essential to protect daily operations of everything in modern life from basic business activity to hospitals to critical infrastructures of nations and the industrialized world.

Every advancement in attacks and in security defined clear generations of evolution. Today IT security deployed by businesses is at a very concerning inflection point because most IT security infrastructures are only at the 2nd and 3rd generation of security while today's attacks are far more advanced 5th generation. Simply put, business's security is behind and ill-equipped to protect against the level of attacks being launched today. After many generations and many products, the "point solution" model of security is operationally heavy and more fragile and cannot be advanced at the same rate of attacks. This is an alarming problem that must first be recognized and then resolved. This new generational model reveals obvious shortcomings in today's security compared to the attacks. So, along with the security rule of thumb to "protect an asset according to its value," this state of affairs calls for another rule of thumb that "the generation of security deployed must at least equal the generation of attacks being launched."

Specifically, to protect against the 5th-generation of attacks, businesses must deploy 5th-generation security. 5th-generation security is advanced threat prevention that uniformly prevents attacks on a business's entire IT infrastructure of networks, virtual instances, cloud deployments, endpoints, remote offices and mobile devices with a single, central management for administration, monitoring and response. It is a foundation that not only protects against 5th-generation attacks but is also an architecture upon which businesses can easily and efficiently add security capabilities as attacks advance and IT environments evolve.

This is Check Point Infinity. Check Point Infinity is a security architecture that delivers advanced threat prevention to protect a business's entire IT infrastructure including all networks, cloud instances and mobile devices against the most advanced attacks of today. The Infinity architecture supports real integration of third-party products and through the Check Point OpSec technology partner program, Check Point offers an incredibly rich ecosystem of supported products. Last, as we've just read, most businesses are unable to continue adding more products to keep up with the rate of advancement of attacks. Infinity addresses this too because it was specifically designed and built to adapt to protect new technologies and forms of attacks.

This is 5th-generation security: Check Point Infinity, the architecture and solution to protect businesses right now, and into the future.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233