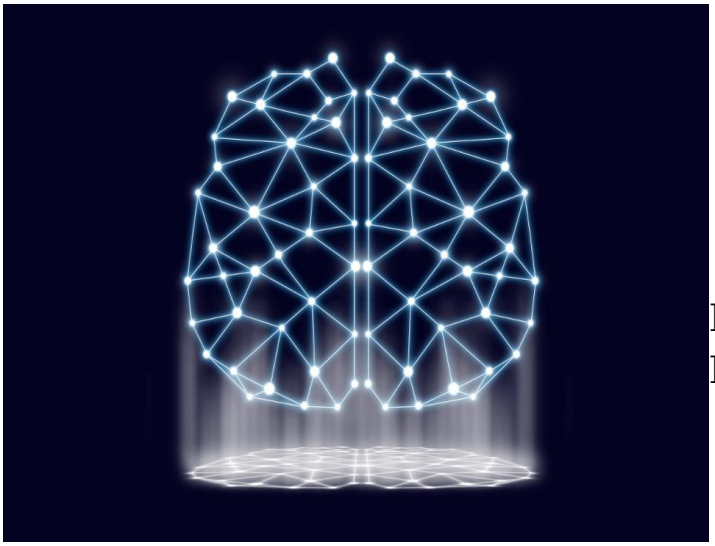
Vector Intelligent System

The most powerful Artificial Intelligence System

Vector is a new technology developed inside an incredible operating System, all advanced feautures are provided by an Artificial Intelligence called “SONIC” in this paper I explain the potentials of this incredible technology .

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com



DIFFERENCE BETWEEN A.I. AND MACHINE LEARNING

Artificial Intelligence (AI) and Machine Learning (ML) are two very hot buzzwords right now, and often seem to be used interchangeably.
They are not quite the same thing, but the perception that they are can sometimes lead to some confusion. So I thought it would be worth writing a piece to explain the difference.
Both terms crop up very frequently when the topic is Big Data, analytics, and the broader waves of technological change which are sweeping through our world.
In short, the best answer is that:
Artificial Intelligence is the broader concept of machines being able to carry out tasks in a way that we would consider “smart”.
And,
Machine Learning is a current application of AI based around the idea that we should really just be able to give machines access to data and let them learn for themselves.

Early Days
Artificial Intelligence has been around for a long time – the Greek myths contain stories of mechanical men designed to mimic our own behavior. Very early European computers were conceived as “logical machines” and by reproducing capabilities such as basic arithmetic and memory, engineers saw their job, fundamentally, as attempting to create mechanical brains.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

As technology, and, importantly, our understanding of how our minds work, has progressed, our concept of what constitutes AI has changed. Rather than increasingly complex calculations, work in the field of AI concentrated on mimicking human decision making processes and carrying out tasks in ever more human ways.
Artificial Intelligences – devices designed to act intelligently – are often classified into one of two fundamental groups – applied or general. Applied AI is far more common – systems designed to intelligently trade stocks and shares, or manoeuvre an autonomous vehicle would fall into this category.

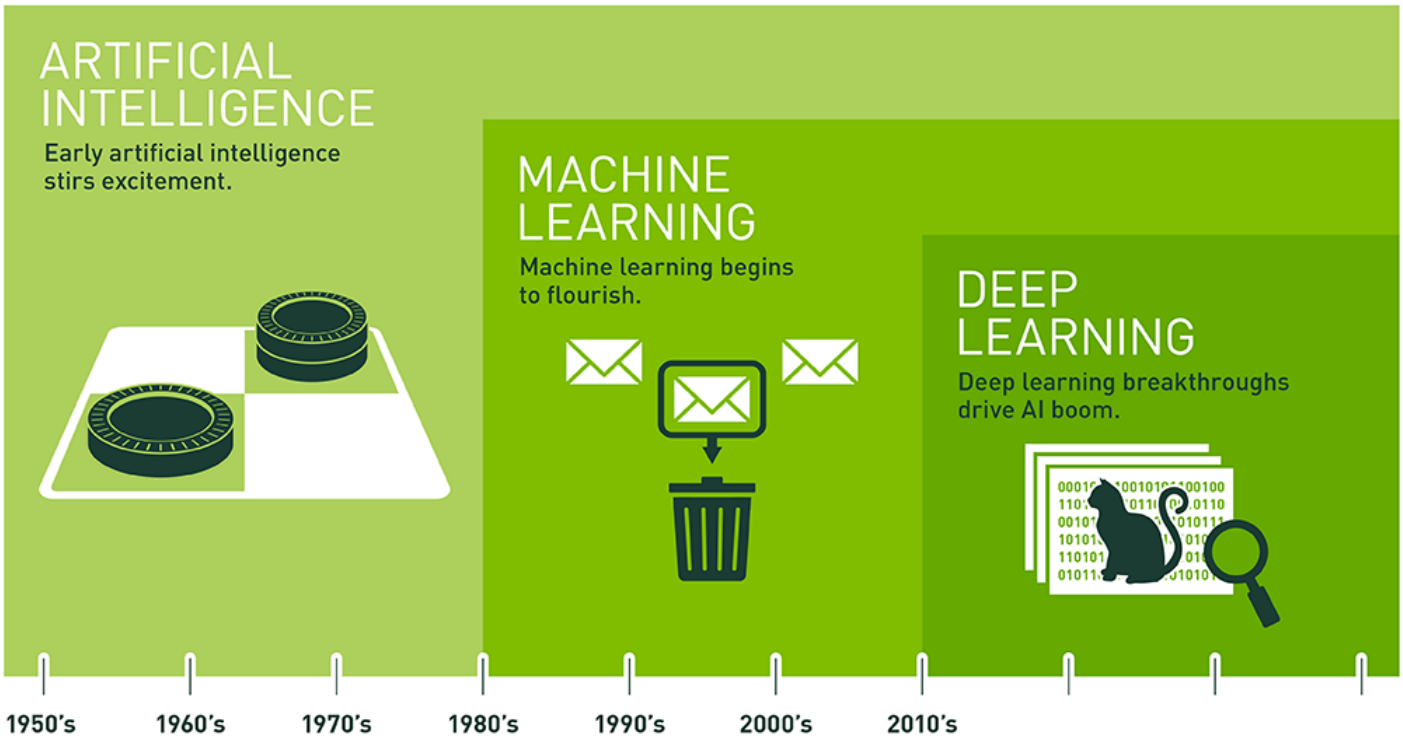
The development of neural networks has been key to teaching computers to think and understand the world in the way we do, while retaining the innate advantages they hold over us such as speed, accuracy and lack of bias.

A Neural Network is a computer system designed to work by classifying information in the same way a human brain does. It can be taught to recognize, for example, images, and classify them according to elements they contain. Essentially it works on a system of probability – based on data fed to it, it is able to make statements, decisions or predictions with a degree of certainty. The addition of a feedback loop enables “learning” – by sensing or being told whether its decisions are right or wrong, it modifies the approach it takes in the future.
Machine Learning applications can read text and work out whether the person who wrote it is making a complaint or offering congratulations. They can also listen to a piece of music, decide whether it is likely to make someone happy or sad, and find other pieces of music to match the mood. In some cases, they can even compose their own music expressing the same themes, or which they know is likely to be appreciated by the admirers of the original piece.
These are all possibilities offered by systems based around ML and neural networks. Thanks in no small part to science fiction, the idea has also emerged that we should be able to communicate and interact with electronic devices and digital information, as naturally as we would with another human being. To this end, another field of AI – Natural Language Processing (NLP) – has become a source of hugely exciting innovation in recent years, and one which is heavily reliant on Machine Learning.

The classic concept of Artificial Intelligence is outdated and is possible to

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

create a relationship between A.I. , Machine Learning and Deep Learning to create an ecosystem that allow to perform the best advanced Data Analysis, the easiest way to think of their relationship is to visualize them as concentric circles with AI — the idea that came first — the largest, then machine learning — which blossomed later, and finally deep learning — which is driving today's AI explosion — fitting inside both.



Since an early flush of optimism in the 1950s, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

But if more people try to combine these feautures for scientifics approaches, for Computer Science or mathematical purpouse etc nobody thinks that 3 law of asimov rules says that “A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws” , so we can use this law to create an advanced deep security systems that combine Active Defence solutions , Endpoint Protection and all feautures about Artificial Intelligence studies together on the same enviroment . But how is possible ? The answer is only one….

VECTOR

Vector is the ultimate security system, all you want inside a unique powerfull Operating System, it focuses its power on an incredible set of components called “OLYMPUS” that grants for single users, companies (smalls, middles and larges), banks, crytical infrastructures and defense systems a 360° solution that evolves in real time and without any human interaction.Vector is the result of years of study and technical analysis to evaluate the real cyber

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

threats by querying all archives (cve , cvs , 0day , Microsft bullettins etc) that newtork administrators use against cyber criminal , but is only one in thousands of options for Vector and I a begin of a new world A REAL SAFE WORLD.

Olympus is the centre of all feautures inside VECTOR but effectively to make the magic of totally and always evolved impenetrability the core of system is the Deep Learning Artificial Subroutine that transforms all informations in a operative strategy, I named this SONIC.

SONIC

SONIC is not a simple defense mechanism, IS ALL YOU WANT AND MORE because the entire VECTOR infrastrucrure is created to continuously evolve in the time without voluntarily commands by administrator.

Why this ? To show the purpouse of this strategy I need to explain the methodology used to create the platform , all based on my personal experiences obtained during my long career of penetration tester , white hat and cyber security

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

experts for all kind of infrastructures . I have to thank my experiences in the field of military cyber security that open my mind to understand that the cyber world is on the threshold of the abyss of the totally computer anarchy and we need a help , a partner that grants a full power control over the network against the people that thinks the net like a world without rules , where you can violate not only systems but human actors , where a bad person can destroy your life and remain umpunished, but this time may finish and the key of this change is VECTOR .

Sonic become works on dynamic threats and is able to adapt to the security measures deployed by users and organizations to combat cybercrime.

In this context, one major challenge is unquestionably the classification of malware. The malware that seems to be “fashionable” today is already obsolete tomorrow and is replaced by another one with completely different or improved features.
At the same time, the newest varieties of malware continue to coexist with older forms, which are still used by cyber criminals without the means to innovate. Therefore, classification in the cybercriminal ecosystem is very complex.

One of the best feauture is that it makes it possible to learn from this dynamism in real time and develop new classification criteria without human intervention. Thanks to this, detection and classification become much more efficient and proactive.

At the same time, its applications are infinite, for example, we also use SONIC together with our development of identification based on biometric behavior. This allows us to rapidly recognize whether a person is interacting with their computer or it is a bot, or if there is a cybercriminal attempting a user or interacting with a user’s account from anywhere in the world.

Machine learning is a key technology in the Sonic System security with a multi-layered approach to protecting endpoints and systems against different threats, blending traditional security technologies with newer ones and using the right technique at the right time.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

For over 5 years I’ve increased the power of machine learning to eliminate spam emails, calculate web reputation, and chase down malicious social media activity and Sonic is the best product because has the ability to auto-develope the latest machine learning algorithms to analyze large volumes of data and predict the maliciousness of previously unknown file types.

THE HUMAN VULNERABILITY

The worst vulnerability that affects all systems is always the human factor , the weak that all attackers plan to create all malicious campaigns.

Most Operating Systems try to abstract human factor from main systems operations for example an abstraction for protection is the execution of an application program with restricted rights allowing a safe communication between hardware and critical systems components. OS tracks program

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

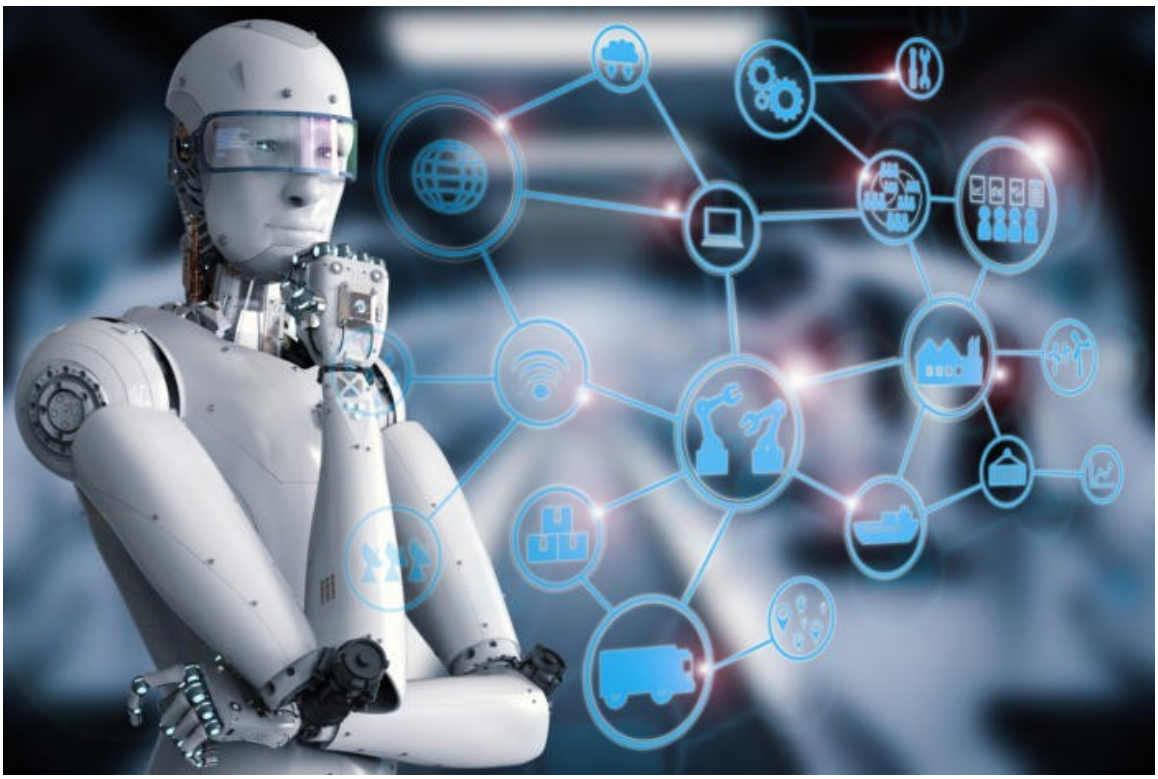
counter and process has a stack that forces OS to track stack pointer and Process Control Block (PCB) Data (program instructions, stack & heap) inspects memory metadata is in PCB etc, but this doesn’t resolve the problem.

Attackers can bypass ASLR AND DEP , Attackers can execute theyr malwares using DPCs (Defferred Procedures Calls) , or use ram to avoid ids control because a standard operating systems DOESN’T HAVE THE TOTAL CONTROL OF ITSELF.

A little example , how you can protect yourself if your arms are blocked?, you can use legs but your body have the full power with a complete control , if anyone may exclude one of these capabilities nobody is completely safe, well this is the principe that inspired me to create a full protection sytems that put itself on the centre of security strategies .

But how can exclude human factors and mantaining the possibility for an administrator or officier or single user to perform all operations on the same time ?

To resolve this probem i’ve created a systems that learn the human behavior step by step and especially by adapting all aspects of systems with the synergistic alaysis of human needs, the centre of the security remain the users protection but for the first time OS is the only root user .



Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

The work for SONIC is so hard because the possibilities of human reactions are infinite and unpredictable but a valid help is the use of Big Data Analysis .

The world of cybersecurity benefits from the marriage of machine learning and big data. As the current cyberthreat environment continues to expand exponentially, organizations can utilize big data and machine learning to gain a better understanding of threats, determine fraud and attack trends and patterns, as well as recognize security incidents almost immediately — without human intervention this is possible by using the powerful of Big Data to perform data mining and improve the security system’s performance.

For me was very important the collaboration with Hadoop developers to help improve its security model. Hadoop is a popular big data framework used by giant tech companies such as Amazon Web Services, IBM, and Microsoft

Machine learning is a useful cybersecurity tool — but it is not a silver bullet. While others paint machine learning as a magical black box or a complicated mathematical system that can teach itself to generate accurate predictions from data with possible false positives.

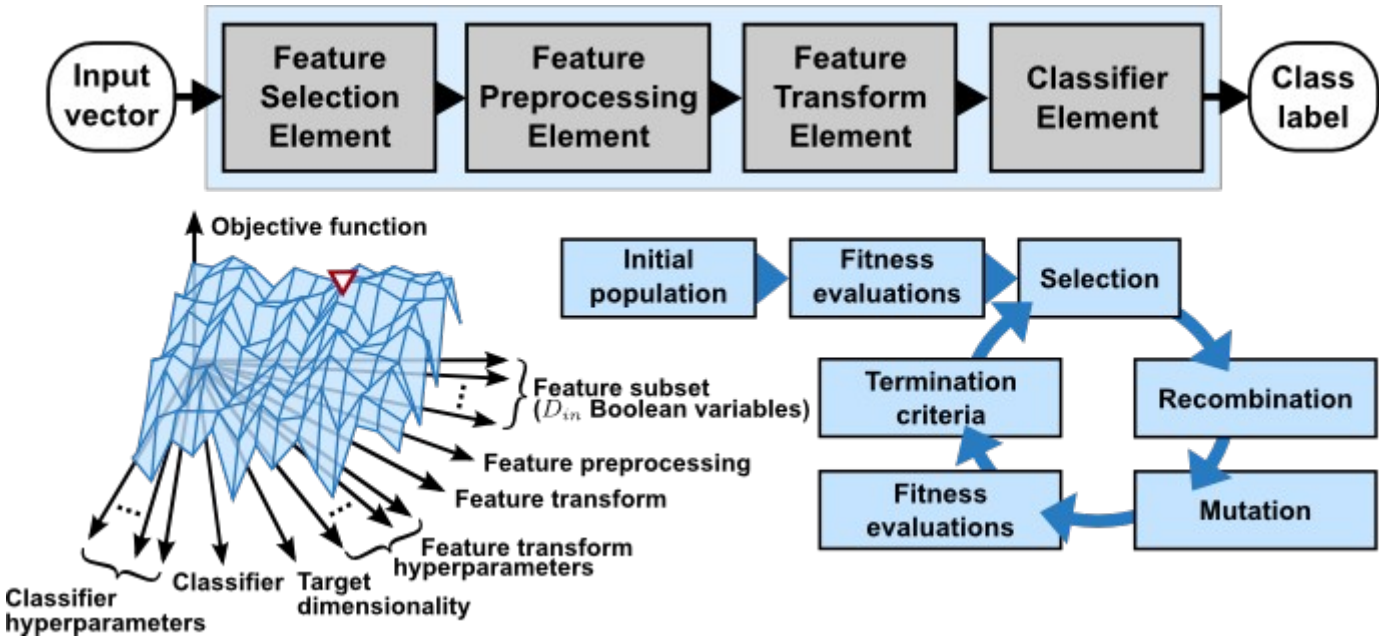
Machine learning has its strengths. It is effective in catching ransomware as-it-happens and detecting unique and new malware files. It is not the sole cybersecurity solution, however. Trend Micro recognizes that machine learning works best as an integral part of security products alongside other technologies.

Sonic takes steps to ensure that false positive rates are kept at a minimum.

Employing different traditional security techniques at the right time provides a check-and-balance to machine learning, while allowing it to process the most suspicious files efficiently.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Dynamical Machine Learning



Sonic uses a dynamical approach to evaluate case by case the right security strategy but how is possible? A possible answer to this question is by use of the Neural Networks.

Artificial Neural Networks, came and mostly went over the decades. Neural Networks are inspired by our understanding of the biology of our brains – all those interconnections between the neurons. But, unlike a biological brain where any neuron can connect to any other neuron within a certain physical distance, these artificial neural networks have discrete layers, connections, and directions of data propagation.

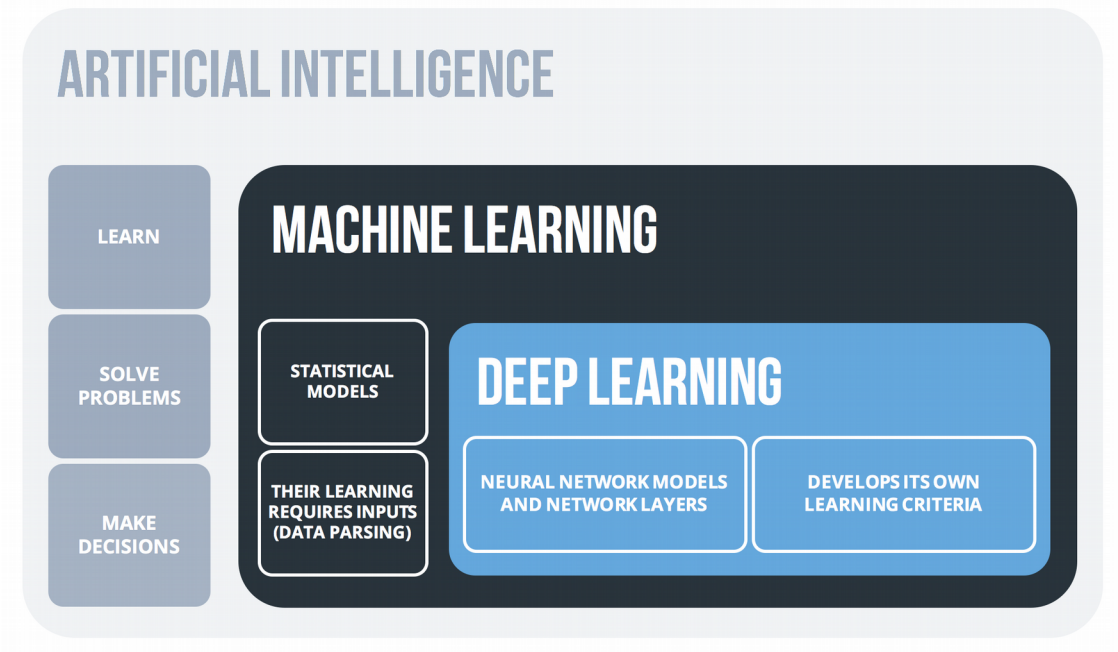
You might, for example, take an image, chop it up into a bunch of tiles that are inputted into the first layer of the neural network. In the first layer individual neurons, then passes the data to a second layer. The second layer of neurons does its task, and so on, until the final layer and the final output is produced.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Each neuron assigns a weighting to its input — how correct or incorrect it is relative to the task being performed. The final output is then determined by the total of those weightings. So think of our stop sign example. Attributes of a stop sign image are chopped up and “examined” by the neurons — its octogonal shape, its fire-engine red color, its distinctive letters, its traffic-sign size, and its motion or lack thereof. The neural network’s task is to conclude whether this is a stop sign or not. It comes up with a “probability vector,” really a highly educated guess, based on the weighting. In our example the system might be 86% confident the image is a stop sign, 7% confident it’s a speed limit sign, and 5% it’s a kite stuck in a tree ,and so on — and the network architecture then tells the neural network whether it is right or not.

The core of Vector’s technologies is the use of the Complex System model that allows the security components to interact with applications and all tasks created by users during every execution. In many cases it is useful to represent such a system as a network where the nodes represent the components and the links their interactions.

Vector Complex systems modules are systems whose behavior is intrinsically difficult to model due to the dependencies, relationships, or interactions between their parts or between a given system and its environment. Systems that are "complex" have distinct properties that arise from these relationships, such as nonlinearity, emergence, spontaneous order, adaptation, and feedback loops, among others. Because such systems appear in a wide variety of fields, the commonalities among them have become the topic of their own independent area of research, the use of Neural Networks allow all user to work in a secure enviroment with the constant protection of SONIC .



Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Total Software Control

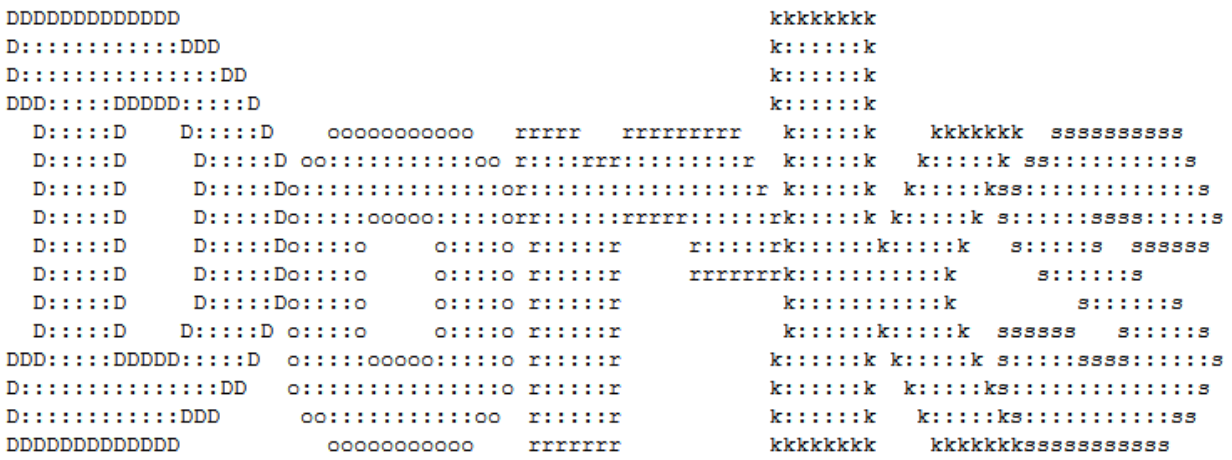
If human factors are the key of a successful client side attacks , at the second place I put certainly the application’s vulnerabilities.

Many developers work to perform the best experience for the users with all possibles security modules (End point protections , ips , ids , firewall etc) that effectively reduce the risk of cyber intrusion but not always is the cure-all.

VECTOR uses SONIC feautures to track all applications activities in real time , for my personal experience of intrinsically safe analysis is very important to create a white list of softwares that firewall and anti virus allow to operate on a traditional operating system , but this method is deprecated and now I prefer to demand the artificial intelligence to continuously extend the white list whit all possible softwares that circulating on the net .

I know it sounds like science fiction but if your system uses the principle of Passive and Active reconnaissance used on penetration testing all is possible but especially all possible threats are predictable .

Google Dorks and Complex Systems



Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Remember that Google is the Oracle , in ancient greece the Oracle was the source of all informations , the genesis of any ideas and the ispiration of any leader , and now ? WE HAVE THE BIGGEST ARCHIVE IN THE WORLD AND WE DON’T USE THIS TREAUSURE TO INCREASE THE KNOWLEDGES OF OUR SYSTEMS??.

A Google dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find

information that is not readily available on a website.

Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search

queries. That description includes information that is not intended for public viewing but that has not been adequately

protected.

As a passive attack method, Google dorking can return usernames and passwords, email lists, sensitive documents,

personally identifiable financial information (PIFI) and website vulnerabilities. That information can be used for any

number of illegal activities, including cyberterrorism, industrial espionage, identity theft and cyberstalking.

A search parameter is a limitation applied to a search. Here are a few examples of advanced search parameters:

site: returns files located on a particular website or domain.

filetype: followed (without a space) by a file extension returns files of the specified type, such as DOC, PDF, XLS and INI. Multiple file types can be

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

searched for simultaneously by separating extensions with “|”.

inurl: followed by a particular string returns results with that sequence of characters in the URL.

intext: followed by the searcher’s chosen word or phrase returns files with the string anywhere in the text.

Multiple parameters can be used, for example, to search for files of a certain type on a certain website or domain. The

Public Intelligence website provides this example:

“sensitive but unclassified” filetype:pdf site:publicintelligence.net

A search parameter is a limitation applied to a search. Here are a few examples of advanced search parameters:

site: returns files located on a particular website or domain.

filetype: followed (without a space) by a file extension returns files of the specified type, such as DOC, PDF, XLS and

INI. Multiple file types can be searched for simultaneously by separating extensions with “|”.

inurl: followed by a particular string returns results with that sequence of characters in the URL.

intext: followed by the searcher’s chosen word or phrase returns files with the string anywhere in the text.

Multiple parameters can be used, for example, to search for files of a certain type on a certain website or domain. The

Public Intelligence website provides this example:

“sensitive but unclassified” filetype:pdf site:publicintelligence.net Those search parameters return PDF documents on that website’s servers with the string “sensitive but unclassified” anywhere in the document text.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Access to internal documents can yield further sensitive information. For example, document metadata often contains more information than the author is aware of, such as revision history, deletions, dates and author / updater names. Because an intruder with the requisite know-how and / or tools can access such information, it’s a good practice to ensure that it is actually removed from documents before they are published or shared. The practice of document sanitization is designed to make sure that only the intended information can be accessed.

In August 2014, the United States Department of Homeland Security (DHS), the FBI and the National Counterterrorism Center ssued a bulletin warning agencies to guard against the potential for Google dorking on their sites. One of the first intrusion prevention measures proposed is to conduct Google dorking expeditions using likely attack parameters to discover what type of information an intruder could access.

But any single possibility doesn’t grant an updated report that helps Artificial Intelligence to provide the best possible result but if you have a complete list?

Well Vector use a powerfull Data Mining solution that scans the global network h24 to find whatever information useful to increase the big knowled of SONIC , for example it scans

Wikipedia

Exploit-db

Google query

Github

And is is a sample inerents the dorks searching , but the data mining approach of vector aimed at increasing the feautures by using all possible informations , for this specific purpouse i’ve created a powerfull algorithm for data (and coin) mining and I called this ICARUS

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

ICARUS

ICARUS uses the power of data mining with the scientific approach of Complex System Analysis, the target of this solution is to avoid that system uses recursively informations that break the line of continuity of machine learning approach.

ICARUS algorithm is chiefly concerned with the behaviors and properties of systems. A system, broadly defined, is a set of entities that, through their interactions, relationships, or dependencies, form a unified whole. It is always defined in terms of its boundary, which determines the entities that are or are not part of the system. Entities lying outside the system then become part of the system's environment.

A system can exhibit properties that produce behaviors which are distinct from the properties and behaviors of its parts; these system-wide or global properties and behaviors are characteristics of how the system interacts with or appears to its environment, or of how its parts behave (say, in response to external stimuli) by virtue of being within the system. The notion of behavior implies that the study of systems is also concerned with processes that take place over time (or, in mathematics, some other phase space parameterization). Because of their broad, interdisciplinary applicability, systems concepts play a central role in complex systems.

As a field of study, complex systems is a subset of systems theory. General systems theory focuses similarly on the collective behaviors of interacting entities, but it studies a much broader class of systems, including non-complex systems where traditional reductionist approaches may remain viable. Indeed, systems theory seeks to explore and describe all classes of systems, and the invention of categories that are useful to researchers across widely varying fields is one of systems theory's main objectives.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

As it relates to complex systems, systems theory contributes an emphasis on the way relationships and dependencies between a system's parts can determine system-wide properties. It also contributes the interdisciplinary perspective of the study of complex systems: the notion that shared properties link systems across disciplines, justifying the pursuit of modeling approaches applicable to complex systems wherever they appear. Specific concepts important to complex systems, such as emergence, feedback loops, and adaptation, also originate in systems theory.

For this ICARUS uses a module that i called "The Survival's rules" :

Complexity

Systems exhibit complexity when difficulties with modeling them are endemic. This means their behaviors cannot be understood apart from the very properties that make them difficult to model, and they are governed entirely, or almost entirely, by the behaviors those properties produce. Any modeling approach that ignores such difficulties or characterizes them as noise, then, will necessarily produce models that are neither accurate nor useful. As yet no fully general theory of complex systems has emerged for addressing these problems, so researchers must solve them in domain-specific contexts. Researchers in complex systems address these problems by viewing the chief task of modeling to be capturing, rather than reducing, the complexity of their respective systems of interest.

While no generally accepted exact definition of complexity exists yet, there are many archetypal examples of complexity. Systems can be complex if, for instance, they have chaotic behavior (behavior that exhibits extreme sensitivity to initial conditions), or if they have emergent properties (properties that are not apparent from their components in isolation but which result from the relationships and dependencies they form when placed together in a system), or if they are computationally intractable to model (if they depend on a number of parameters that grows too rapidly with respect to the size of the system).

Networks

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

The interacting components of VECTOR system form a network, which is a collection of discrete objects and relationships between them, usually depicted as a graph of vertices connected by edges. Networks can describe the relationships between individuals within an organization, between logic gates in a circuit, between genes in gene regulatory networks, or between any other set of related entities.

Networks often describe the sources of complexity in complex systems. Studying complex systems as networks therefore enables many useful applications of graph theory and network science. Some complex systems, for example, are also complex networks, which have properties such as power-law degree distributions that readily lend themselves to emergent or chaotic behavior. The fact that the number of edges in a complete graph grows quadratically in the number of vertices sheds additional light on the source of complexity in large networks: as a network grows, the number of relationships between entities quickly dwarfs the number of entities in the network.

Nonlinearity

A sample solution in the Lorenz attractor when $\rho = 28$, $\sigma = 10$, and $\beta = 8/3$

Complex systems often have nonlinear behavior, meaning they may respond in different ways to the same input depending on their state or context. In mathematics and physics, nonlinearity describes systems in which a change in the size of the input does not produce a proportional change in the size of the output. For a given change in input, such systems may yield significantly greater than or less than proportional changes in output, or even no output at all, depending on the current state of the system or its parameter values.

Of particular interest to complex systems are nonlinear dynamical systems, which are systems of differential equations that have one or more nonlinear terms. Some nonlinear dynamical systems, such as the Lorenz system, can produce a mathematical phenomenon known as chaos. Chaos as it applies to complex systems refers to the sensitive dependence on initial conditions, or "butterfly effect," that a complex system can exhibit. In such a system, small

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

changes to initial conditions can lead to dramatically different outcomes. Chaotic behavior can therefore be extremely hard to model numerically, because small rounding errors at an intermediate stage of computation can cause the model to generate completely inaccurate output. Furthermore, if a complex system returns to a state similar to one it held previously, it may behave completely differently in response to exactly the same stimuli, so chaos also poses challenges for extrapolating from past experience.

Emergence

Another common feature of complex systems is the presence of emergent behaviors and properties: these are traits of a system which are not apparent from its components in isolation but which result from the interactions, dependencies, or relationships they form when placed together in a system. Emergence broadly describes the appearance of such behaviors and properties, and has applications to systems studied in both the social and physical sciences. While emergence is often used to refer only to the appearance of unplanned organized behavior in a complex system, emergence can also refer to the breakdown of organization; it describes any phenomena which are difficult or even impossible to predict from the smaller entities that make up the system.

One example of complex system whose emergent properties have been studied extensively is cellular automata. In a cellular automaton, a grid of cells, each having one of finitely many states, evolves over time according to a simple set of rules. These rules guide the "interactions" of each cell with its neighbors. Although the rules are only defined locally, they have been shown capable of producing globally interesting behavior, for example in Conway's Game of Life.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Spontaneous order and self-organization

When emergence describes the appearance of unplanned order, it is spontaneous order (in the social sciences) or self-organization (in physical sciences). Spontaneous order can be seen in herd behavior, whereby a group of individuals coordinates their actions without centralized planning. Self-organization can be seen in the global symmetry of certain crystals, for instance the apparent radial symmetry of snowflakes, which arises from purely local attractive and repulsive forces both between water molecules and between water molecules and their surrounding environment.

Adaptation

Complex adaptive systems are special cases of complex systems that are adaptive in that they have the capacity to change and learn from experience. Examples of complex adaptive systems include the stock market, social insect and ant colonies, the biosphere and the ecosystem, the brain and the immune system, the cell and the developing embryo, manufacturing businesses and any human social group-based endeavor in a cultural and social system such as political parties or communities.

These are standards rules but with combined work between SONIC and ICARUS you can transform your system in an incredible security machine .

ACTIVE DEFENSE

If you consider that WannaCry ransomware attack in May 2017 and the NotPetya attack in June 2017 offer cases in point. In each, hackers helped themselves to tools stolen from intelligence agencies and others and created havoc around the world, forcing systems

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

off-line at the Chernobyl nuclear power station, affecting several parts of Britain's National Health Service, and interrupting scores of computer systems. The relatively unsophisticated nature of the attack limited the overall take. Yet, it reveals just how vulnerable organizations are to even rudimentary hacks done at scale. Imagine if the attackers actually had their acts together.

Some do. Several of the world's best-protected organizations have been attacked over the past few years, including a number of preeminent government agencies and technology companies. Hackers who may once have been groping around in the dark are acquiring a deeper understanding of who they're targeting and how to get inside. Thanks to a proliferation of botnets1 and the easy sharing of tools on the dark web, the expense of mounting cyberattacks is also plunging. Put it all together, and criminals, some of whom are state sponsored, have ready access to cash, technologies, and resources. Over the coming years, crimes in the cyberrealm are predicted to cost the global economy $445 billion annually.2

Perversely, the high-profile hacks may have done us a favor. For a long time, cybersecurity experts have proselytized about the evolving threat landscape. But like doctors who caution their patients to avoid sedentary lifestyles, the risks these experts describe seem important but distant. The WannaCry attack—its brazenness, the speed at which it scaled, and how effortlessly it derailed business as usual—took cyberthreat activity from a slow-moving abstraction and made it real.

Businesses must consider themselves warned. Rather than continue in a passive stance, organizations must adopt an "active defense" model: they should assume their firewalls will be penetrated. They should assume that encryption keys will be compromised, and that hackers will stay a step ahead of them in deploying malware in their infrastructure. Active defense requires organizations to anticipate attacks before they happen, detect and respond in real time, establish traps and alarms to contain attacks, and adopt a tiered approach to protecting critical assets.3

Understanding the challenges

The threat environment is constantly changing, but how businesses have responded to

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

those threats has remained largely the same. That's not going to work anymore. Here's why:

A significant number of breaches are still caused by employee lapses. Despite years of training employees on good data-hygiene practices and continued investment in malware and virus detection, the majority of corporate data breaches are caused by simple human error: clicking on an innocent-seeming email, downloading a legitimate-looking attachment, or revealing identifying information to a seemingly trustworthy source.4 Even if two-thirds of employees avoid these traps, about one-third will still fall prey (and about 15 percent of this group will go on to become repeat victims).5 That means an automated barrage like a phishing campaign that blasts messages to thousands of employees is assured a reliable percentage of hits—and this is just by using basic techniques. More devious attackers can do extensive damage. All it takes is one or two employees to expose their credentials, and an attacker can decrypt them and make their way inside. Most organizations are not set up to thwart this behavior.

Perimeter and encryption defenses aren't enough. Large organizations have spent millions on firewalls and encryption. But the strongest perimeter defenses won't keep a company safe if intruders are already inside—and given the earlier point regarding internal threats, businesses must assume some are. Once there, intruders can stay for months, acquiring information and using that information to enter the systems of other companies. Criminals know that the best targets are well defended, so rather than trying to penetrate a heavily secured front door, they can go around to the back, to the company's supply chain. Data show that 63 percent of data breaches come from exploiting weak points in a company's customer and vendor network.6 One major consumer-goods chain, for instance, suffered a major loss when attackers climbed in through the proverbial ducts by hacking the company's air-conditioning vendor and working their way in. Companies need to do more than bar the gates; they need to monitor their entire network (and, in some cases, their network's network) to anticipate where attacks will come from. But most organizations don't have that capability.

IT organizations are overwhelmed and underresourced. Challenging the IT and security organization to keep up with the latest attacker moves is unfeasible. After all, hackers may only need a blunt tool and a few resources to exact a toll on one target. IT

organizations meanwhile have to stay alert to thousands of external threats from a variety of sources. They need to be able to filter out the most pertinent intelligence, and have a sufficiently detailed understanding of where their most critical data assets are stored as well as what could put those assets at risk to secure them properly—all while continuing to support the IT needs of the entire business. Trying to manage all these demands can lead to indecision and conflicting priorities. An effective response requires expertise and capabilities to detect, deter, and defend against these risks. But while some companies, such as large banks and telecommunications organizations, have been able to build credible defenses at that scale, the spending level required can stretch to the hundreds of millions. Few organizations can match that.

We are likely to have more malicious actors entering the field, more attacks that take advantage of basic loopholes, and more players capable of launching sustained, pernicious insider-based attacks. New strategies and partnerships are required.

Shifting to an active-defense model

Active defense allows organizations to engage and deflect attackers in real time by combining threat intelligence and analytics resources within the IT function. The approach draws upon lessons the military community learned in defending itself in fluid attack environments like Afghanistan and Iraq. To ferret out and respond to risks faster, commanders began positioning operators, planners, and intelligence analysts in the same tent where they could feed special operations teams with ongoing, real-time information. Integrated and more accurate intelligence made it easier for units to track chatter, identify targets, and increase the number of missions they could conduct over the course of an evening.

In recent years, some large organizations have applied that thinking to bolster their own defenses. A major financial-services institution, for instance, greatly enhanced its cybersecurity capabilities by convening a team dedicated to providing active defense. The team established state-of-the-art threat-monitoring capabilities so it could continually scan the company’s ecosystem—its own network as well as the broader supply chain—for unusual patterns and activity, sniff out potential threats, and thwart attacks, often within minutes of detection. It has impeded thousands of attacks as a result.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Few organizations have the budget to build dedicated centers of this scale. But there are other ways to access needed capabilities. By realigning the existing budget, engaging outside resources, and forging information-sharing partnerships, businesses can still mount a strong active defense. Success in doing so starts with understanding what's involved. Here are the central elements of an active defense posture:

Sonic has the power to anticipate attacks before they happen. If the old model was all about defending the organization with layers of perimeter protection, the new model is far more proactive. Businesses need to scour the threat environment to find out if someone is talking about them or someone in their chain, pinpoint software and network vulnerabilities, and spot potential hacks before they occur. This is an intelligence-heavy, data-driven process—and it's critical. Bringing cybersecurity experts into the tent can help organizations gain the insights needed. Third parties that specialize in threat intelligence monitor a wide range of sources. That includes following threads and conversations in places like the dark web—websites that require special software to access and provide user anonymity—to gauge evolving threats to the company or its vendors.

Detect and respond to attacks in real time

Early detection depends on an organization's ability to track network patterns and user behavior that deviate from the norm. The challenge is to figure out what normal is, given that businesses are constantly changing and human behavior is unpredictable. Intrusion detection and anomaly detection are two widely used approaches. Intrusion-detection systems (IDS) look for misuse based on known attack patterns. However, because these systems are trained to spot defined threat signatures, they may miss emerging ones. They may also have a hard time distinguishing problematic activity from legitimate activity, such as innocuous internal communications that contain flagged language or Internet addresses (for example, malware warnings), ongoing network-security-vulnerability scans, or attacks against systems that have already been patched. Anomaly-detection models work the other way around. Instead of looking for known attack signatures, they look for behavior that deviates from typical network patterns, such as an

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

unusual spike in volume. Companies with an active defense posture use both IDS and anomaly-defense systems to provide more comprehensive threat detection.

Establish traps and alarms to contain attacks. Decoy servers and systems, known as deceptions, are another tool that companies can deploy as part of their active defense. Deceptions lure attackers into a dummy environment where they can be studied to gain additional intelligence. Entrance into the trap sets off an alarm, alerting the threat-operations center and triggering software agents and other deterrents to be placed in the network to close off access and prevent damage to the business. Some businesses also salt these environments with false information to confuse attackers. Once intruders breach a system, they usually return through the same gateway. Deceptions and other traps need to be convincing enough facsimiles to keep intruders inside long enough for the company to gather useful insights. Companies can then use those repeat visits to record the methods attackers are using to gain file, system, or server access and update their defenses accordingly.

Use ring architectures to protect critical assets

Over the longer term, businesses need to construct layers of defense to keep the company's most critical assets deeply buried. Ring architectures, for instance, allow organizations to store data in different layers depending on the value and sensitivity of those assets. Each layer requires a specific key and authorization protocol to manage access. Penetration in any one layer will set off alarms. Active defense also requires an IT plan that organizes and prioritizes security-related technology spending. Otherwise, it can be tempting to try to protect everything and in the end create vulnerabilities when spending and systems prove too difficult to maintain.

Taken together, these measures can make a profound difference. At one financial institution, for instance, intelligence gathered on the dark web revealed that an overseas criminal syndicate was seeking to access the credentials of the bank's high-net-worth clients. Analysts informed their IT counterparts, all of whom worked together in an integrated active-defense unit. Engineers spotted command-and-control-type traffic emanating from PCs associated with high-income zip codes and found a pattern of anomalous log-ins for some of their high-net-worth accounts. The threat center

immediately activated a forced password reset for affected customer accounts and placed temporary holds on all wire transfers in excess of $100,000. In addition, it reimaged affected desktops and issued a communication to select high-net-worth customers, encouraging them to implement two-factor authentication. This quick, coordinated response prevented sensitive information from being compromised.

Using this average skills when a threats was detected SONIC activate an evolution of dionaea honeypot called NEMESYS (my personal nickname on the net) that use the most advanced protocols used on labrea and dionaea honeypots :

- blackhole
- epmap
- ftp
- http
- memcache
- mirror
- mqtt
- mssql
- mysql
- pptp
- sip
- smb
- tftp
- upnp

but in addition of these protocols i’ve created a super secret protocol that i’ve called ODINO .

ODINO is a evolution of tarpit function , his target is not only the less of cyber criminal activities , for the first time YOU HAVE A COMPLETE HACKING SOLUTION USED BY AN

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

INCREDIBLE ARTIFICIAL INTELLIGENCE.

The results is that when your enterprise is attacked , SONIC not only protects your infrastructures but on the same time , attacks with all possible exploit the attacker machine , THE BEST DEFENSE IS ALWAYS A GOOD OFFENSE.

OPEN ZFS SOLUTION

ZFS is significantly different from any previous file system because it is more than just a file system. Combining the traditionally separate roles of volume manager and file system provides ZFS with unique advantages. The file system is now aware of the underlying structure of the disks. Traditional file systems could only be created on a

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

single disk at a time. If there were two disks then two separate file systems would have to be created. In a traditional hardware RAID configuration, this problem was avoided by presenting the operating system with a single logical disk made up of the space provided by a number of physical disks, on top of which the operating system placed a file system. Even in the case of software RAID solutions like those provided by GEOM, the UFS file system living on top of the RAID ransform believed that it was dealing with a single device. ZFS's combination of the volume manager and the file system solves this and allows the creation of many file systems all sharing a pool of available storage. One of the biggest advantages to ZFS's awareness of the physical layout of the disks is that existing file systems can be grown automatically when additional disks are added to the pool. This new space is then made available to all of the file systems. ZFS also has a number of different properties that can be applied to each file system, giving many advantages to creating a number of different file systems and datasets rather than a single monolithic file system.

The use of ZFS allows VECTOR to create a multipartition Operating System that decentralized the access of all data sources to improve the maximum data protection and use mongo db data replication (only on the servers) to grant the availability of data for a long time .

Constant Updated NO OS CHANGE

Like a Human VECTOR has the possibility to upgrade itself indipendently and without any human interaction , vector use a new algorithm to edit your personal repository by adding a new packet softwares that internet offers day by day.

All is possible because vector doesn’t derive from any OS , it has a new revolutionary kernel built on top of actually technology

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Finance

Evolution. That is the key to define the current situation about online banking fraud. As specialist, we are aware that in the vast majority of case, the cybersecurity discipline acts in a reactive way againts the threats of cybercriminals. A very typical way of acting in the banking sector. Let's give a simple and very typical example, a cybercriminal desing a cybercriminal designs a phishing campaign to steal online banking credentials.

Usually, after the detection of online fraud, an approach is made to close the portal where the malicious files reside, to use blacklists published by antivirus manufacturers, modify the rules and configurations, warn the user of which has been infected, etc. Each company develops its own techniques with tools and processes to face these types of situations. Despite all the efforts, online banking fraud continues to increase:

•More and more banks are using this type of platform to reach their customer. The increase is due to the speed and ease to carry out frequent operations like transfers, know the balance, etc.

•The cybercrime sector has become a very lucrative sector, reaching to coin the name "crime-as-a-service".A situation that allows each cyber criminal to specialize in each process of the criminal chain, such as the development of complex techniques to infect a user and rob him of his bank credentials. The more specialized the cybercriminal, the more elaborate and innovative their techniques will be.

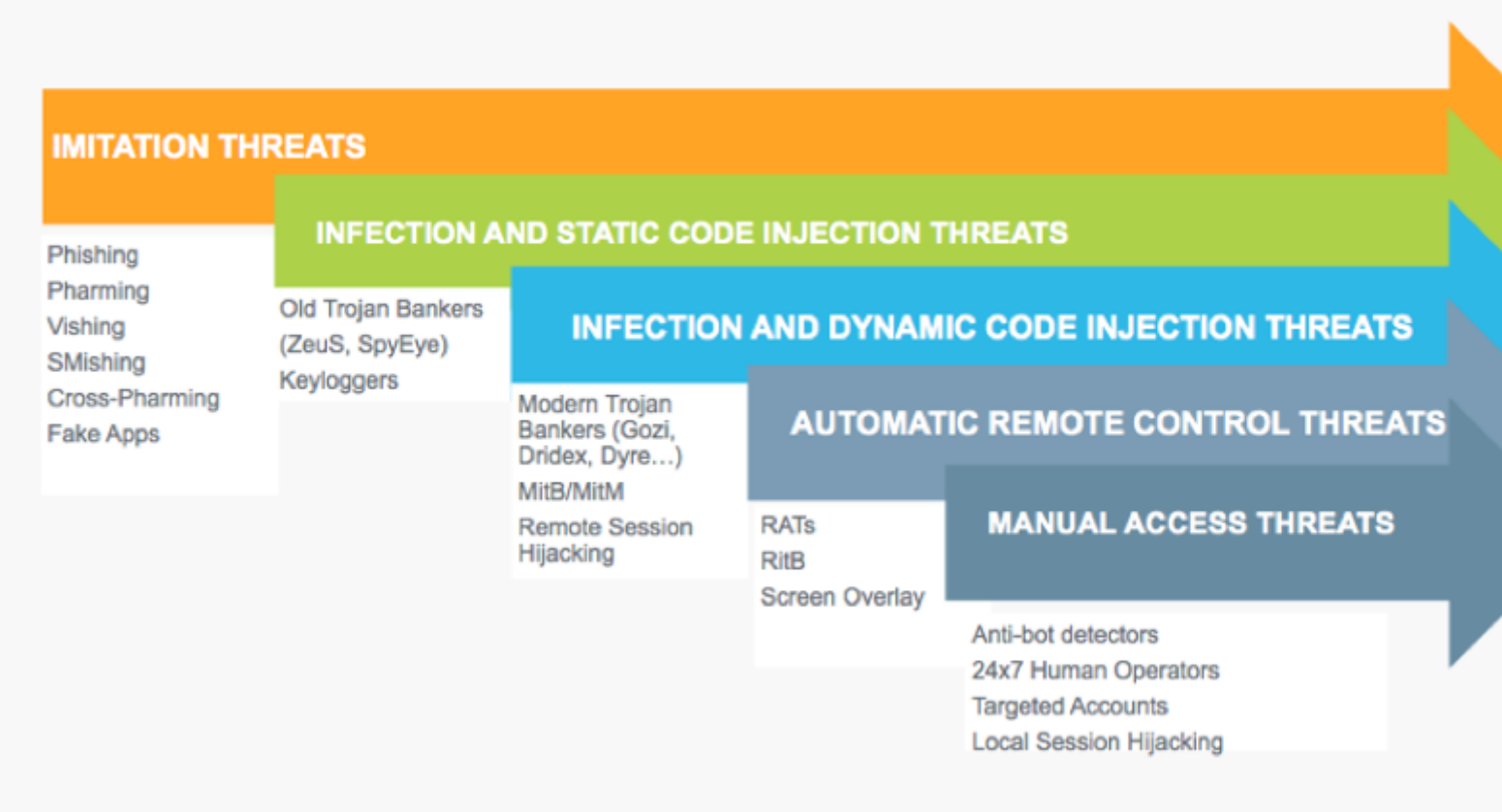
•Bank fraud provides quick returns with a low level of risk, since criminal cyber identification is complex and time consuming. For criminals, online banking represents a great business opportunity.

•New cybercrime patterns appear that allow you to circumvent with relative ease at any time during the session of the user. For example RAT, Account Take Over, bots, Man-in-the-Browser (MitB), etc.

•Finally, users who demand the services of online banking often lack sufficient security measures to combat these patterns.

Today, the main challenge facing banks is to be able to acquire a thorough knowledge of the new techniques, tactics and procedures (TTP) of cybercriminals to quickly generate the new threats. In buguroo we consider that the techniques and tactics of online banking fraud are currently organized into three categories:

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com



Threats Based on Imitation

Imitation threats, most commonly known as phishing and their variances (Vishing, SMishing, etc.), are the oldest and through the use of sophisticated social engineering techniques redirect users to sites that are copies of legitimate bank sites.

These fake sites run on different infrastructures from legitimate ones and eventually try to get sensitive user information. Some phishing and ransomware attacks also affect legitimate banking mobile apps (fake apps).

Infection and Injection Threats

The most dangerous and recent threats are dynamic infections and injections, which actually change legitimate websites to deceive the user. Once the user's machine is infected by malware, fraudsters update the malware remotely and dynamically add new features or bank sites for which the malware can inject code.

This way, fraudsters through the use of dynamically generated Command & Control Servers, can easily update their botnets increasing the list of potential banks to attack and code injections by using latest toolkits delivered in the Black Market, therefore maximizing their chance to commit fraud with low exposure.

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

Automatic Remote-Control Threats

Automated Remote Control threats take control of an online banking session after the user has been authenticated with an authorized device. Fraudsters often use commercial software for remote control or malware specifically designed for this purpose. These attacks are especially dangerous because they combine multiple techniques, such as blocking sessions with a web injection and manipulating account balances in the background with a RAT.

Fraudsters can purchase services from botnet operators that monitor account balances and create automatic mechanisms to take manual control over user accounts. Besides all these techniques, there are always situations where fraudsters or mafias directly bribe or even blackmail internal bank employees as to get banking sensitive client information.

Actually banks use this security methods:

•Lack of Visibility to Improve Protection
•Current Market Solutions Rarely Detect Emerging Threats
•Ensuring Protection with no impact to User Experience
•Banks Have a Huge Attack Surface
•False Positives are an Extended Problem

How to face the chagenller?

Sonic Money is the next generation of Bank Security System for mobile and web applications that helps banks protect online users. When a user accesses his online account, Sonic Money profiles four layers of data while maintaining data privacy compliance:

•Biometry: identifies the user’s biometric behaviour and cognitive analytics to uniquely profile each human behind a device
•Web contents: checks the information a user displays to detect if it’s being manipulated by third-party attackers, without false positives or negatives
•Environment: profiles the user’s context information such as devices, network, and geo-location and crosses it with threat intelligence data to identify anomalies in the user’s environment
•Omni-channel: correlates data from multiple inputs, such as web browsers, mobile devices, and application servers to make sure solution is not bypassed by attackers

Sonic Money then process and analyses all these indicators in order to make sure it detects new emerging threats eventually covering all 3 types of threats mention earlier (even those frauds based on blackmailing or bribing internal banking employees) and

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

provide this information to the bank in real time without any possible interactions by officers, SONIC will be your best protection system , your best friend that forever serve the people against all types of cyber criminals.

Secret feautures

This is only a little view of VECTOR possibilities , but the the truth is that VECTOR has an hidden power that transform this system in a real military resource on the combat zone and for governement to increase the power of IoT smart grid surveillance.

The hidden power of vector is stored in a kernel substrate called ADE that allows the system to exploit a simple principle already known to DARPA but effectively never diffused , but with my personal skills acquireds during my studies and in real life cyber operations i’ve created a complete solution that will put on the top of Military Machine Learning System.

There are several possible applications withVECTOR for the military. Replacing frozen software with systems that do not need to be refreshed periodically creates a broad potential for creating more nimble systems, possibly at lower cost. Again, AI could be used in training systems. It provides an unpredictable and adaptive adversaries for training fighter pilots (VECTOR Simulator) it understands photos and videos and cans greatly help in processing the mountains of data from surveillance systems or for “pattern-of-life” surveillance. Facial recognition Ais inside VECTOR called IRIS can be used to close “skill gaps” in complex maintenance it enables systems to interact with humans using natural language. VECTOR NLP (Natural Language Processor) could enable systems to take orders without using keyboards. It also can translate documents and could serve as a translator in the future.

And is in not all VECTOR uses ICARUS to perform the best quantum uses the advanced principles of quantum computing to give ICARUS the possibility to realize quantum mining capable of increasing performance both in terms of cryptocurrencies mining

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com

and high frequency trading of 10000% and sincerely I have not been able to simulate the potentials at full capacity of my algorithm so I hope to be able to test the huge potential of my system in front of the right audience and with the right infrastructure.

THIS IS ONLY AN ANTICIPATION

IF YOU WANT TO KNOW THE REAL POWER OF THIS SYSTEM...

giovanni.chiara@pec.ordineavvocaticatania.it

tel: 095 533178

Developer: James Ferrara
Contact: +39 3476133225
giaco.ferra83@gmail.com