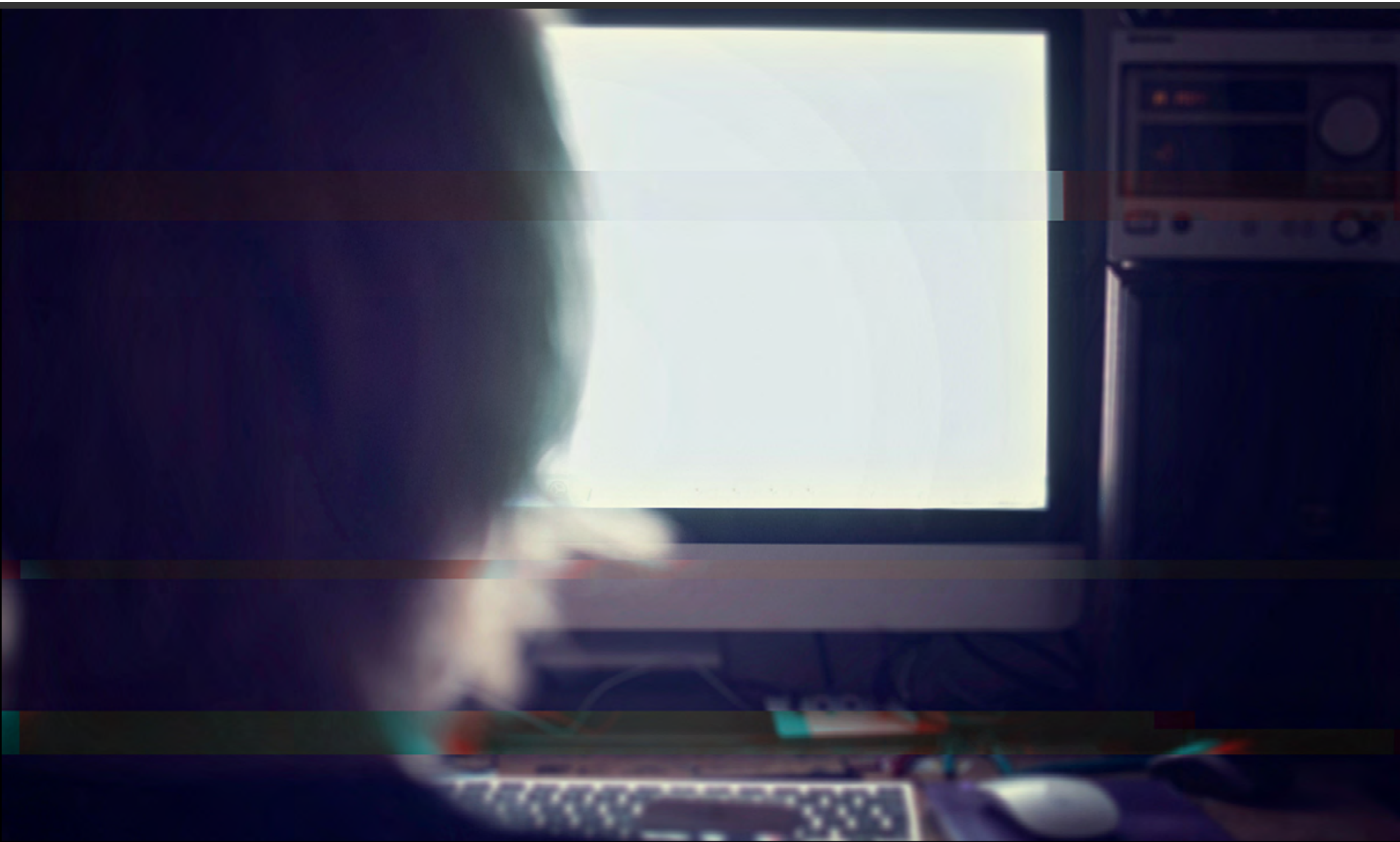
ARMOR™

BETWEEN YOU AND THE THREAT

Evolution of the online battlefield

A BRIEF HISTORY OF THE CYBER THREATS & THE EMERGENCE OF THE APT DESIGNATOR

DR. CHASE CUNNINGHAM | **DIRECTOR, CYBER THREAT RESEARCH & INNOVATION**





Foreword

Portions of the following research were originally published as part of my doctoral dissertation in Computer and Information Systems Security/Information Assurance at Colorado Technical University. It explores the genesis of advanced persistent threats (APT) and how they now occupy mainstream awareness.

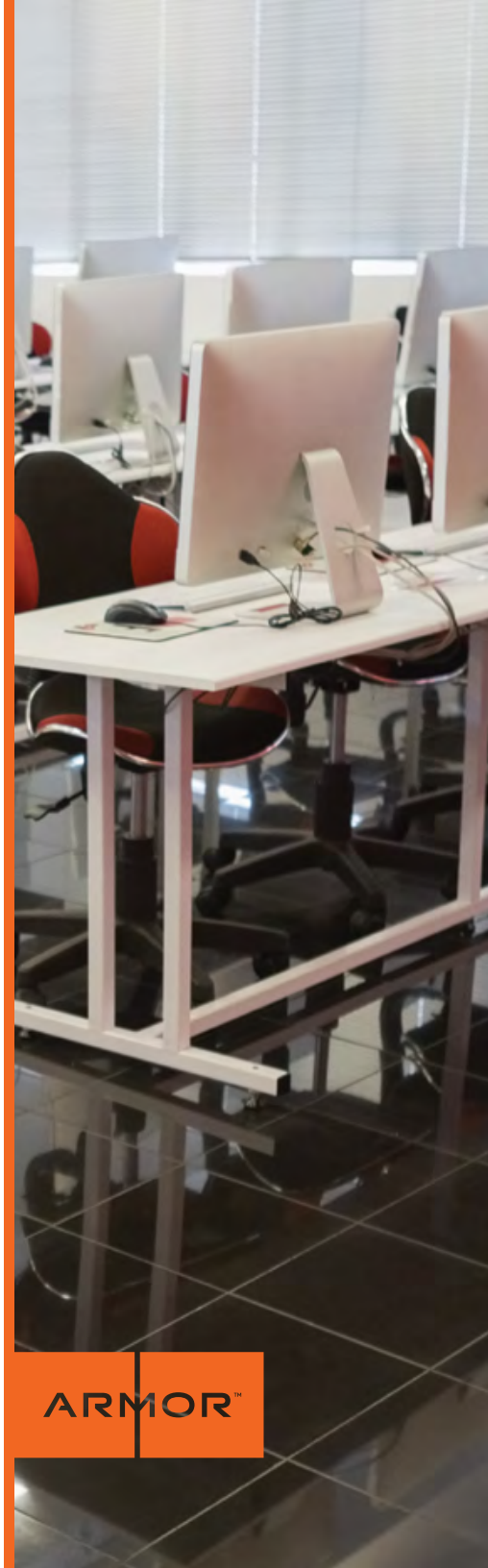
Outside of project research, the full study is the longest and often most taxing component of the doctoral journey. The program's dissertation committee is constantly reviewing the material to uncover holes in the concepts, themes and understanding presented. The objective is to validate the author as an expert in his or her topic area — both historically and via reviewed literature (the latter not included with this publication).

I hope you find the discussion enlightening and it provides valuable context for how threats have evolved to permeate today's online landscape.

Dr. Chase Cunningham
Director, Cyber Threat Research & Innovation | Armor







Cybersecurity retrospective

Computer security, and the study of computer threats and exploitation, has not always been at the forefront of computer science. The first real instance of computer threat research and exploitation studies actually began during the 1970s and was not even related to computers.

Instead, the studies were noted as a problem in the telephone-switching network. The phone system was growing so fast and becoming so large that the system had to be integrated and automated to survive.

This first automated phone system was built to serve a large test environment and immediately many problems were discovered. Calls originated and ended on their own, phone numbers were allocated to persons without phones, and myriad other issues came to light. These initial issues were not actually considered threats, but rather problems for the owners of the systems and those administering the networks.

In the 1980s, the modem became the powerhouse for connecting and managing the large networks that were becoming more and more commonplace and, as such, modems became the primary point of compromise from which systems could be hacked.

"The first real instance of computer threat research and exploitation studies actually began during the 1970s and was not even related to computers."

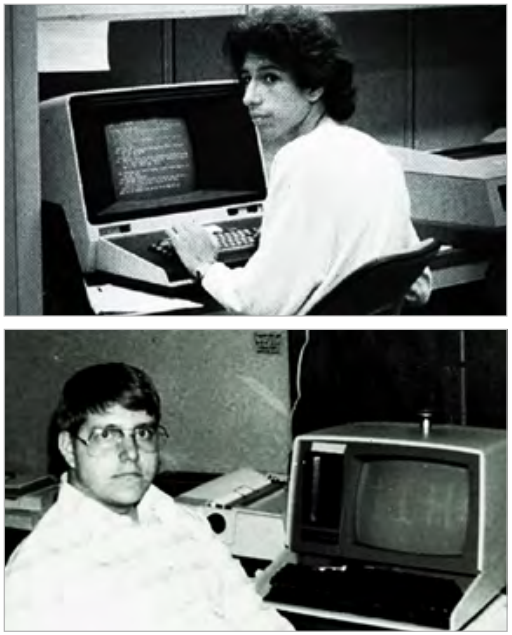


The 414 code

While there are many different opinions about the first real virus on a computer system, the reality of this becoming a problem for computers did not become prevalent in public literature until the computer became a household item in the mid-1980s. During the "age of modems," groups like the 414s — a collection of modem hackers named for their Milwaukee, Wisc., area code — were identified and arrested by the FBI (Hansman, 2003).

The 414 group targeted the phone networks and modems of Los Alamos National Laboratory and a center for cancer research using a combination of malicious code and a deep understanding of the flaws in the automation technology that was used by the phone companies.

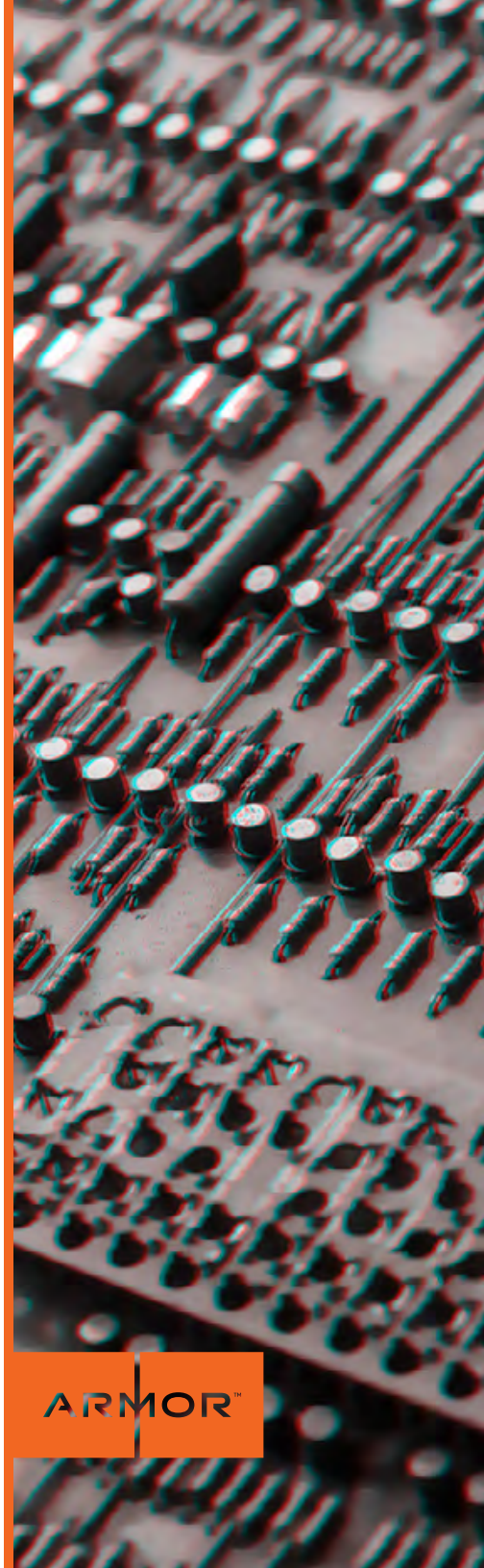
Not long after this first noted computer threat campaign was finalized, the federal government passed the Computer Crime and Abuse Act in 1986 (CISPA, 2010). This legislation detailed what constituted a protected computer and the resulting punishment for those who sought to conduct malicious actions against any protected system (Grance, Kent & Kim, 2004).



Neal Patrick, top, and Timothy Winslow, bottom, were original members of the 414s in the early 1980s.

1982 | 1983 | 1984 | 1985 | 1986

1983 The reality of the computer virus in popular culture becomes prevalent with the 414s, a group of modem hackers who leveraged an understanding of flaws in the automation technology used by phone companies.



Birth of cybersecurity research

Only a few innovative and industrious companies understood the possible maliciousness that could be wrought by activities such as those being conducted by hackers and nefarious groups.

Consequently, it was during this time that companies like Symantec and IBM began to actually research and study viruses and malware to isolate and mitigate threats.

The malware and anti-virus company McAfee was established during this era. John McAfee noticed that many of his friends' and associates' computers were acting abnormally and running very slowly.

After some research, he was able to discern that programs had either been installed and were intentionally causing detriment to the system, or that programs had begun to simply degrade and harm the system on which they were running.

After some technical research and development, McAfee was able to write specific technical signatures for the anomalies within those programs. The signature-focused malware and anti-virus system was born (Hutchins, Cloppert & Amin, n.d.). McAfee's system of signature recognition and anomalous behavior detection was immediately recognized as a pivotal point in mitigating and detecting these newly recognized threats.

Overnight, companies began to follow suit.



John McAfee founded computer anti-virus company McAfee Associates in 1987.

1986 | 1988 | 1989 | 1990

1987 McAfee founded McAfee Associates, a computer anti-virus company. McAfee pioneers the cybersecurity industry by developing a signature-focused malware and anti-virus system.



Growing government involvement

It was not until 1987 that the U.S. federal government began to notice this type of activity and institute the first Computer Emergency Response Team, today commonly known as CERT (Grance et al., 2004).

By the early 1990s, the rate of annual computer virus detection grew to more than 1,000 per month. As the detection and isolation of computer viruses became an actual practice area within computer science, the detection and signature generation for viral programs also increased exponentially.

By 1995, more than 250,000 viruses — or variances of viruses — had become commonplace. All of these incidents, early exploits and attacks paled in comparison to the growth of cyber threats that emerged in the early 21st century.

The field of specific targeted cyber threats, especially cyber threat research, did not truly exist prior to the early 2000s. The first mentions of cyber threats and cybercrime appeared in 2001 during an unclassified briefing from the National Security Agency (Werlinger, Muldner, Hawkey & Beznosov, 2010).

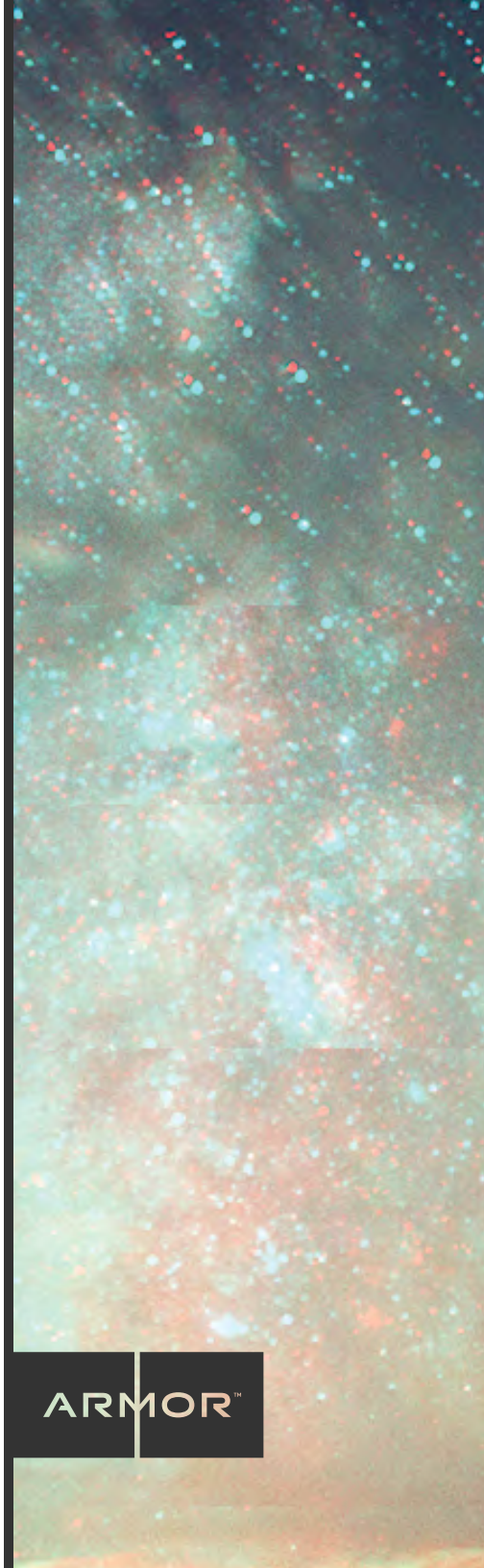
This particular report was solely focused on the issue of securing a network as large as that of the U.S. Department of Defense (DOD). Certain aspects of the report alluded to a highly trained and motivated cyber threat that was likely already deeply embedded in many DOD networks.





1995

More than 250,000 viruses — or variances of viruses — had become commonplace. All of these incidents, early exploits and attacks paled in comparison to the growth of cyber threats that emerged in the early 21st century.



The evolution of APTs

Advanced persistent threats — commonly referred to as APTs today — came to light during a discussion at the U.S. Air Force Intelligence Agency.

The discussion involved a group of lieutenant colonels exploring which term to use to classify the new type of computer hacker — the ones who were very well trained and very successful.

Since these attackers were advanced, persistent and certainly a threat, the term APT was born. The moniker quickly become the industry norm for foreign government cyber operators and skilled threat teams.

While this single term is used to categorize and identify a rather wide swath of possible threats, it is worth noting that APT is now used by almost every cyber warfare magazine and cybersecurity official — from think tanks all the way to the White House.

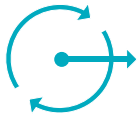
In order to truly be considered an APT-specific attack, there are a few general criteria that are accepted by some, but not all, analytic groups across both industry and cyber operations personnel.

For these groups, the totality of the operation that took place, and the means by which the group conducted the attack, must generally fall into the following three categories for the attack to be even considered as a likely APT attack or exploitation event:

ADVANCED



PERSISTENT



THREAT





2006

The U.S. Air Force is typically credited with the origination of the advanced persistent threat term.



Advanced

Operators behind the threat must have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging.

While individual components of the attack may not be classified as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required.

They often combine multiple targeting methods, tools and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.

Persistent

Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities.

The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful.

If the operator loses access to their target they usually will reattempt access — most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats that only need access to execute a specific task, such as run-of-the-mill hackers and those seeking financial gain via computer hacking.



Threat

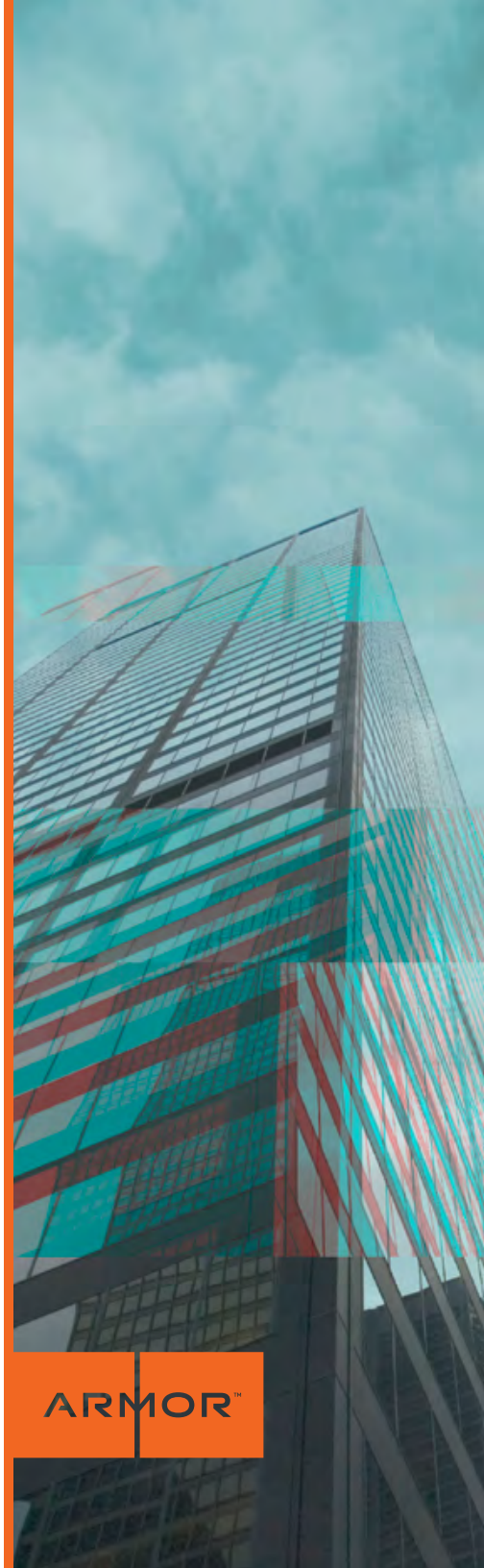
APTs have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code.

The operators have a specific objective and are skilled, motivated, organized and well funded. This funding has typically been known to come from either a host nation's government or from an extremely well-funded nefarious group, such as mafia or crime syndicates.

However, in some cases, there has been an indication that funding may have come from one or more of these providers. There are even cases where the source of funding appears to be interwoven between criminal enterprises and host-nation agents.

APT exploitation and targeting also follows a well-defined methodology and practice of attempting to maintain anonymity both during and following an exploitation or compromise. Again, this is likely due to several factors, the primary of which is that the host nation funding and guiding the operation does not wish to have it known that they are participating in such a covert, and possibly damaging, attack.

However, the above definitions for APT, and the clarification of the usage for this classification of attack, are still not adopted across the entirety of cyberspace. For many different agencies, corporations and governments, the definition of any APT exploitation event is extremely difficult to concretely define.



Analyzing APTs

Consider that an organization such as NATO has more than 28 different countries working within its combined operations center. Each one of these different groups has been actively targeted and independently hacked or exploited by different APT groups and actors.

However, there had been literally no reporting criteria or vehicles across NATO that succinctly and definitively detailed the need for an APT designation. Each country and group reporting or analyzing their relative exploitation event determined APT differently.

Even within different agencies of the U.S. government, attempting to specifically detail an APT exploitation event or hack cannot be done well. The NSA has its own specific set of criteria for determining an APT attack. Meanwhile, the CIA and FBI have their own criteria. At the time of original publication, none of these cross-referenced each other and none possessed the same rules for declination.

The lack of a cohesively uniform definition for APT operations and exploitation provides a great example of just how fluid and dynamic this area of study currently is and has been.

Further, this example shows how the lack of group-think and broad term definition is so prevalent within cyber operations and analysis that even defining one of the most important terms used in the industry is difficult at best. It's almost impossible to clearly identify and isolate any one threat group; the generic APT term is used across such a wide spectrum.

"It's almost impossible to clearly identify and isolate any one threat group; the generic APT term is used across such a wide spectrum."

In the mid-to-late 2000s, a large section of the computer and Internet industry was focused solely on increasing the speed and interoperability of its networks and usability of its products, all while paying little, if any, real attention to security or cyber threats.

It wasn't until the discovery of a coordinated and large-scale attack that concern for the future of computer security — and later cybersecurity — became a serious consideration for both developers and persons in places of political power.

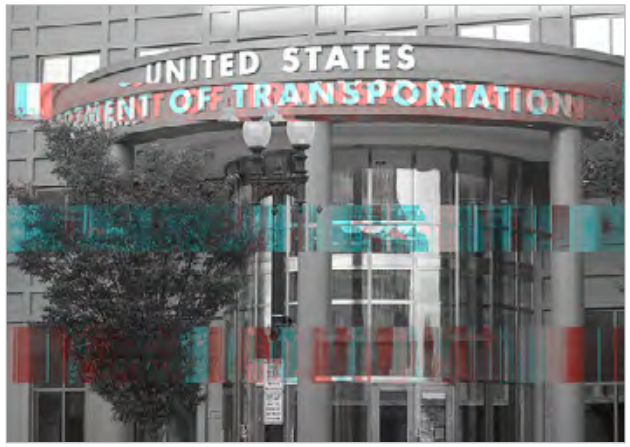


Zeus arrives

This first real cyber threat incident was the discovery of the Zeus botnet in 2007 (Singh & Silakari, 2009). This attack targeted the U.S. Department of Transportation and was responsible for extracting large amounts of data from government systems.

Data ranging from passwords for master control systems and system administrator passwords to network and control mapping systems and proprietary code samples were all taken (Singh & Silakari, 2009).

While there were many previous computer viruses and different variations of computer threats prior to this, the discovery of the Zeus botnet — and the engineering and powerful programming capabilities of those behind the threat group — led the development of a dedicated study of cyber threats into its own area of focus.



2006 | 2008 | 2009 | 2010

2007 The Zeus botnet appears for the first time when it was used to steal sensitive data from the U.S. Department of Transportation.



DDoS leveraged in war effort

In 2007, Russia was engaged in a dispute with the nation of Estonia. While the dispute was not of much international significance, and certainly not of technical or cyber significance, the resulting cyberattack and planning certainly was.

As the political and societal sabers began to increase their rattling, the Russian government began to maneuver its forces into place for an invasion of Estonia. As the actual offensive operations began, nearly every aspect of Internet-based infrastructure in Estonia was attacked by distributed-denial-of-service (DDoS) attacks (Goodchild, 2009).

Everything from banking systems and government websites to state-sponsored media outlets and any other connected system that was of military or strategic importance was taken "offline" by these attacks.

Billions of packets were launched simultaneously from tens of thousands of computers and servers located within and outside of Russia. As the Estonian systems began to crash and communications and coordination were interrupted, the Russian military moved into position and enforced its will on the Estonian government.

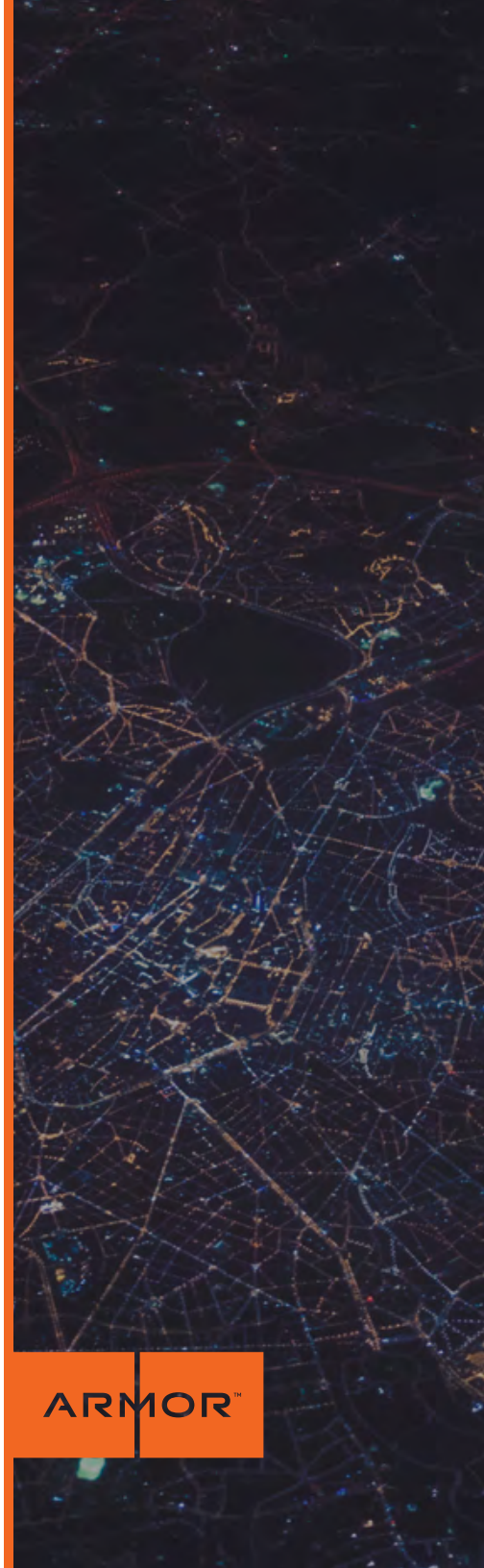
While officially none of the cyberattacks were either attributed to or acknowledged by the Russian military or government, the implications and trail of evidence indicate that a coordinated cyberattack was launched in conjunction with this military operation.

This was one of the first and most powerful examples of how a relatively simple, yet coordinated cyberattack could not only hamper communications, but also severely impede a defended system and cause a real loss of command and control for those under attack.

Two years later, in 2009, the U.S. Department of Defense officially declared cyberspace a war-fighting domain in an effort to ensure an attack such as this could legally be met with reciprocal force (Haack, Fink, Maiden, McKinnon, & Fulp, n.d.).



2007 The Russian government launches a series of DDoS attacks on Estonia. The attacks take out banks, ministries, media outlets and other connected systems of military and strategic importance. The sophistication and military planning behind these attacks were seen as unprecedented.



Defining cyber threats

In more recent history, the definition of cyber threat — and any attempt to systematically or intelligently further demarcate the differences between what constitutes a cyber threat — has become unclear at best.

Consider the use of malware in relation to cybersecurity and cyber threats. While malware is certainly considered a subset of a cyber threat issue, it is not by itself an identifying term.

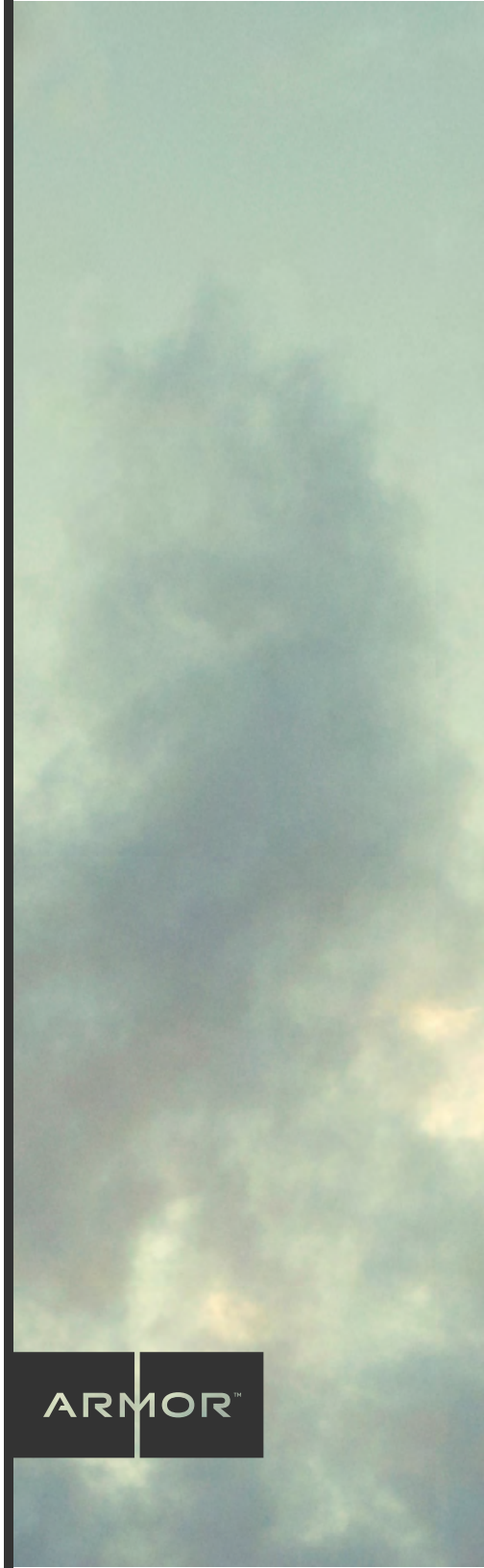
Typically, research and academic work within the cyber field now discuss malware as a piece of the cyber problem. Any research or discussion of the malware term breaks down into an immediate classification of the malware type itself.

In addition, terms and definitions, such as social engineering and exploitation, have become a piece of the collective definition of cyber threat research.

They are not typically considered as specific corollaries to any set of cyber threat groups or certain operations. These terms and their uses, within cyber research, evolve on a nearly daily level and have become more a study of tying specific cyber actions or operations to a group of cyber threats, instead of the collective research determining any with any specificity what certain terms can be tied to which cyber threat.

It is the language equivalent of trying to catch rain in one's hand; the medium simply moves too quickly and is reformed along its own whims.

"It is the language equivalent of trying to catch rain in one's hand; the medium simply moves too quickly and is reformed along its own whims."



Conclusion

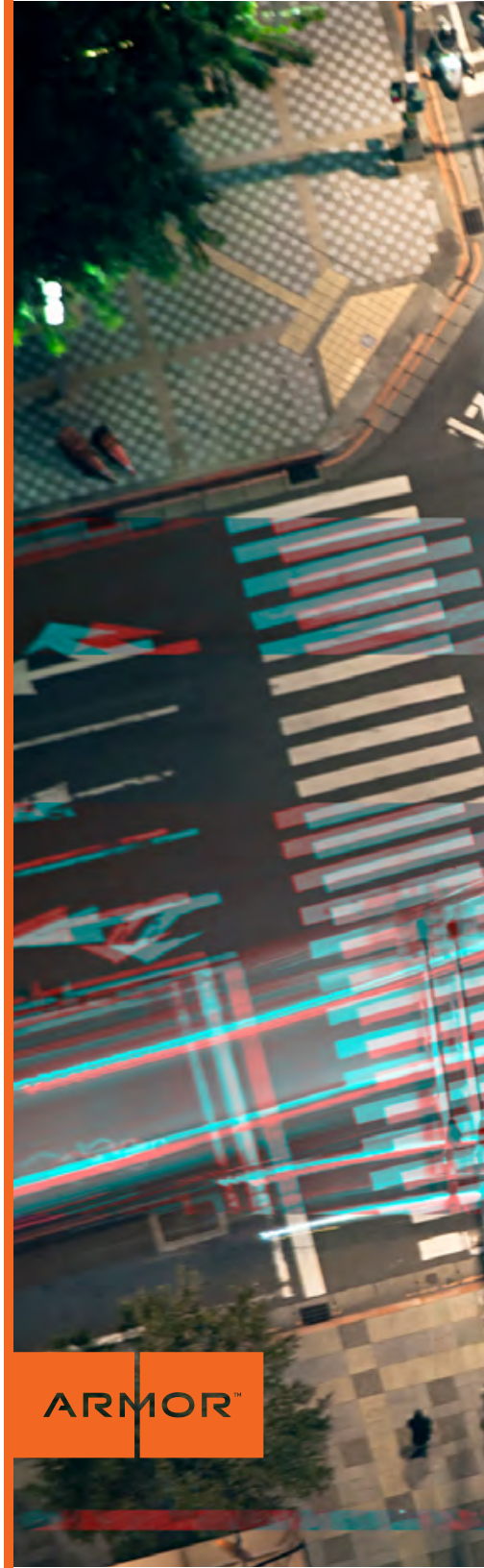
The current threat landscape did not mature overnight. Like many things, it slowly evolved from infancy — learning, adapting and optimizing over the years. Three decades ago, industry leaders couldn't know what was in store for today's online environments.

They were preoccupied with innovation; concepting and building cutting-edge technology, not defending against threats that didn't exist and couldn't be practically realized.

This perspective, however, doesn't alter our current posture. With the provided history of APTs, it's clear to see why our global online community is woefully behind threat actors.

They've enjoyed years to watch, learn, design and test — and most of the time largely undetected.

> "The current threat landscape did not mature overnight. Like many things, it slowly evolved from infancy — learning, adapting and optimizing over the years."



Works Cited

- **Aeran, A. (2006). Comprehensive overview of Insider Threats and their Controls. Royal Holloway.**
  Retrieved from http://www.cccure.org/Documents/Insider%20Threat/InsiderThreatsReport.pdf

- **Bhasin, M. (2007). Mitigating cyber threats to banking industry. Chartered Accountant.**
  Retrieved from http://220.227.161.86/96551618-1624.pdf

- **Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. The Diamond Model of Intrusion Analysis.**
  Center for Cyber Intelligence Analysis and Threat Research Hanover Md, 2013. http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf.

- **Canter, David. "Offender Profiling and Criminal Differentiation." Legal and Criminological Psychology 5, no. 1 (2000): 23-46**

- **Cappelli, D., Moore, A., Trzeciak, R., & Shimeall, T. J. (2009). Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1.**
  Published by CERT, Software Engineering Institute, Carnegie Mellon University, www.cert.org.
  Retrieved from http://www.cert.org/archive/pdf/CSG-V3.pdf

- **Catrantzos, Nick. "No Dark Corners a Different Answer to Insider Threats," 2010.**
  Retrieved from https://calhoun.nps.edu/public/handle/10945/25049

- **Chen, A. (2013, March 1). Why Did Bradley Manning Do It? Gawker. www.gawker.com.**
  Retrieved from http://gawker.com/5987951/why-did-bradley-manning-do-it

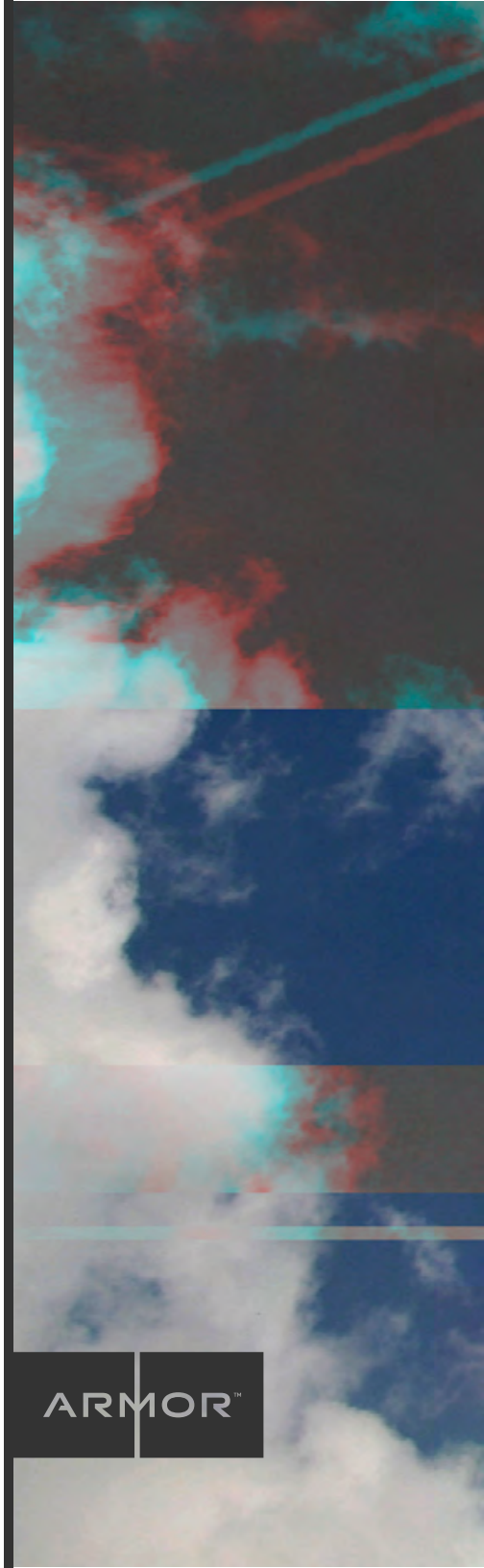
- **Chivers, H., Clark, J., Nobles, P., Shaikh, S., & Chen, H. (2013). Knowing who to watch: Identifying attackers whose actions are hidden within false alarms and background noise.**
  Information Systems Frontiers, 15(1), 17-34. doi:10.1007/s10796-010-9268-7

- **Christodorescu, M., Jha, S., & Kruegel, C. (2008). Mining specifications of malicious behavior.**
  In Proceedings of the 1st India software engineering conference (pp. 5-14). Retrieved from http://dl.acm.org/citation.cfm?id=1342215

- **Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., & Center, C. I. T.**
  (2012). Chronological examination of insider threat sabotage: preliminary observations. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3(4), 4-20.

- **Cohen, T. R., Panter, A. T., & Turan, N. (2013). Predicting counterproductive work behavior from guilt proneness.**
  Journal of Business Ethics, 114(1), 45-53.

- **Donald, E., & Louise, E. (2000). Interactive analysis of computer crimes.**
  Retrieved from http://www.isy.vcu.edu/~gdhillon/Old2/teaching/Spring07-VCU-790-GlobalConseq/temp/Interactive%20analysis%20of%20comp%20crimes%20-%20Computer.pdf



- **Doss, Gary W. "An Approach to Effectively Identify Insider Attacks within an Organization."**
  Ph.D., Nova Southeastern University, 2012. ProQuest Dissertations & Theses Full Text (951851575).
  Retrieved from https://login.ctu.idm/oclc.org/?url=http://search.proquest.com/docview/951851575?accountid=26967

- **Fava, Daniel. "Characterization of Cyber Attacks through Variable Length Markov Models," 2007.**
  http://scholarworks.rit.edu/theses/3113/

- **Felson, Marcus, R. V. G Clarke, Great Britain, Home Office, and Policing and Reducing Crime Unit.**
  Opportunity Makes the Thief: Practical Theory for Crime Prevention. London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 1998.

- **Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks.**
  In Proceedings of the 2007 ACM workshop on Recurring malcode (pp. 1-8). Retrieved from http://dl.acm.org/citation.cfm?id=1314391

- **Gibbs, Graham R. Analysing Qualitative Data. Sage, 2008**

- **Glasser, Joshua, and Brian Lindauer. "Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data,"**
  98-104. IEEE, 2013. doi:10.1109/SPW.2013.3

- **Greitzer, F., & Hohimer, R. (2011). Modeling Human Behavior to Anticipate Insider Attacks.**
  Journal of Strategic Security, 4(2). doi:http://dx.doi.org/10.5038/1944-0472.4.2.2

- **Hanley, M., Dean, T., Schroeder, W., Houy, M., Trzeciak, R. F., & Montelibano, J. (2011).**
  An analysis of technical observations in insider theft of intellectual property cases. DTIC Document.
  Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA549391

- **Hargreaves, Claire, and Daniel Prince. "Understanding Cyber Criminals and Measuring Their Future Activity," 2013.**
  Retrieved from http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf.

- **Holt, T. J. (2013). Cybercrime and criminological theory: fundamental readings on hacking, piracy, theft, and harassment**.
  San Diego, CA: Cognella.

- **Jakobsson, M., & Ratkiewicz, J. (2006). Designing ethical phishing experiments: a study of (ROT13) rOnl query features.**
  In Proceedings of the 15th international conference on World Wide Web (pp. 513-522).
  Retrieved from http://dl.acm.org/citation.cfm?id=1135853

- **Karin Instone - Counterproductive Work Behaviour - White Paper.pdf. (n.d.)**

- **Kim, Do Hoon, and Hoh Peter In. "Cyber Criminal Activity Analysis Models Using Markov Chain for Digital Forensics,"**
  193-98. IEEE, 2008. doi:10.1109/ISA.2008.90

- **Lowman, Sarah. "Criminology of Computer Crime," 2010.**
  http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.391.670&rep=rep1&type=pdf



- **Magklaras, G. B., and S. M. Furnell. "Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse."**
  Computers & Security 21, no. 1 (2001): 62-73.
- **Markh, J. (2009). Computer Forensics Seminar for Week 6: Network Forensics I.**
  Forensic Software Analysis. blog. Retrieved from http://blog.inteliident.com/2011_07_01_archive.html
- **Mount, Michael, Remus Ilies, and Erin Johnson. "Relationship of Personality Traits and Counterproductive Work Behaviors: The Mediating Effects of Job Satisfaction."**
  Personnel Psychology 59, no. 3 (2006): 591-622.
- **Nellikar, Suraj. "Insider Threat Simulation and Performance Analysis of Insider Detection Algorithms with Role Based Models."**
  University of Illinois, 2010. https://www.ideals.illinois.edu/handle/2142/16177.
- **Neufeld, D.J. "Understanding Cybercrime,"**
  1-10, 2010. doi:10.1109/HICSS.2010.417
- **Porras, P., Saidi, H., & Yegneswaran, V. (2009). Conficker C analysis. SRI International.**
  Retrieved from http://cs.uno.edu/~dbilar/11CSCI6621-NetworkSecurity/04.22.11.BotnetsConficker.CSCI6621/An%20Analysis%20of%20Conficker%20C.pdf
- **Raj, V. S., & Chezhian, R. M. (n.d.). A STUDY ON RECENT SOPHISTICATED MALWARES AND ADVANCED THREATS ON CYBERSPACE.**
  Retrieved from http://ijarcce.com/upload/2013/july/11-vyshali%20raj%20-a%20study%20on%20recent%20sophisticated.pdf
- **Rich, Eliot, Ignacio J. Martinez-Moyano, Stephen Conrad, Dawn M. Cappelli, Andrew P. Moore, Timothy J. Shimeall, David F. Andersen, Jose J. Gonzalez, Robert J. Ellison, and Howard F. Lipson. "Simulating Insider Cyber-Threat Risks: A Model-Based Case and a Case-Based Model."**
  In Proceedings of the 23rd International Conference of the System Dynamics Society, 17-21, 2005. ftp://163.25.117.117/gyliao/TODylan/Simulating%20Insider%20Cyber-Threat%20Risks-A%20Model-Based%20Case%20and%20a%20Case-Based%20Model.pdf.
- **Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-reported Deviant Computer Behavior: A Big-5, Moral Choice, and Manipulative Exploitive Behavior Analysis.**
  Deviant Behavior, 27(3), 245-268. doi:10.1080/01639620600605333
- **Rogers, Marcus K. "The Psyche of Cybercriminals: A Psycho-Social Perspective." In Cybercrimes: A Multidisciplinary Analysis,**
  edited by Sumit Ghosh and Elliot Turrini, 217-35. Springer Berlin Heidelberg, 2011. http://dx.doi.org/10.1007/978-3-642-13547-7_14.
- **Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research.**
  In Insider Attack and Cyber Security (pp. 69–90). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-0-387-77322-3_5
- **Shaw, E. D., & Stock, H. V. (2011). Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall. White Paper,**
  Symantec, Mountain View, CA. Retrieved from https://scm.symantec.com/resources/21220067_GA_WP_Malicious_Insider_12_11_dai81510_cta56681.pdf



- **Stermsek, Gerald, Mark Strembeck, and Gustaf Neumann. "A User Profile Derivation Approach Based on Log-File Analysis."**
  In IKE, 2007:258–64, 2007. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.141.6449&rep=rep1&type=pdf

- **Tariq, M.A., J. Brynielsson, and H. Artman. "Framing the Attacker in Organized Cybercrime,"**
  30-37, 2012. doi:10.1109/EISIC.2012.48

- **Vankka, J. (2013). Cyber warfare. National Defence University, Department of Military Technology Series 1: No. 34.**
  Retrieved from https://doria17-kk.lib.helsinki.fi/handle/10024/91529

- **Xua, K., Yaoa, D. D., Pérez-Quinonesa, M. A., Scott, E., & Gellerb, C. L. (n.d.). An Empirical Study on Quantitative Modeling of Adversary's Knowledge.**
  Retrieved from http://people.cs.vt.edu/danfeng/papers/cyber-game.pdf

- **Yaseen, Qussai, and Brajendra Panda. "Insider Threat Mitigation: Preventing Unauthorized Knowledge Acquisition."**
  International Journal of Information Security 11, no. 4 (May 16, 2012): 269-80. doi:10.1007/s10207-012-0165-6.

- **Ye, Nong, and X. Li. "A Markov Chain Model of Temporal Behavior for Anomaly Detection."**
  In Proceedings of the 2000 IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop, 166:169, 2000.
  https://homepages.laas.fr/owe/METROSEC/DOC/WA1_1.pdf



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™
BETWEEN YOU AND THE THREAT

© ARMOR 2016. All rights reserved.