Computational Decoys for Cloud Security

Angelos D. Keromytis Columbia University



Decoys

- Fake objects whose purpose is to deceive adversaries
 - Detection of adversary
 - Diversion (attraction) of effort
 - Harm avoidance
 - Continued misdirection
 - Reach-back



Real Life Decoys

The New York Times				N.Y. / Region					
WORLD	U.S.	N.Y. / REGION	BUSINESS	TECHNOLOGY	SCIENCE	HEALTH	SPORTS	OPINION	
Polic Thie By JOSEP Published:	ce to ves H GOLD	STEIN	ke Pill	Bottles to	Track	Drug	store		
Seekin the <u>Ne</u>	g to ca w Yor	atch and even k Police Depa	tually dete <u>rtment</u> wil	r addicts who s l stock pharma	steal painl cy shelves	killers, s with	FACEB	OOK ER	
decoy	pill bo	ttles that con	tain trackii	ng devices.			👯 ପେଠୁଣା	_E+	

Traditional Cyber Decoys

- Well-known security strategy
 - Honeypots
 - Honey-monkeys (web)
 - Honey-accounts (email spam)



An Evening with Berferd
In Which a Cracker is Lured, Endured, and Studied
Bill Cheswick
AT&T Bell Laboratories
Abstract
January 1991 a cracker, believing he had discovered the famous sendmail DEBUG hole in our laterest g lies, attempted to obtain a conv of our nansword file. I sent him one

success, anonput is come a copy of our password task. I not hall note, The several motivative we do this excision on a morey chaose in order to trace his location and learn his techniques. This paper is a chronicle of the excision 's "successes' and disappointments, the bait and traps used to love and detect him, and the chrone' "fail" we have the such his activities.

We concluded that our ranker had a ke of time and persistence, and a good list of security holes to use once he obtained k logic os a machine. With these both he could often solvert the usey and bis accounts in short setter, and then new. Dur ranker was horsened in sultary targets and new machines to help lauded his consections.

1. Introduction

Our secure linemet gateway was firmly in place by the spring of 1990(1). With the castle gate in place, I wondered are often the lock was tried. I have there were behaviours outdraw, Who was they? Where dd hay attack from on draw other? What security holds did life yit? They weren't fooding and starget and ATAT, nerety Shaffang with the door. The altimate flaw would be to limit a cracker into a situation where we log his sessions, have a thing or two, and was his subsequent tegrin.

The overe of an average vertraining on the literark has few tools for sarvering bare queriess. Conservation years done and repert one product, but ingome to done, year query was a producing 40 mergahyes of donained logs each day for the standard services. How often were people trying to see the services well not support? We added a few faite services, and 1 wents a script to scare the logs daily. This lise of services and other lares has grown—serve one date the following:

PTP: The scatter produces a report of all logit names that were assempted. It also reports the use of a tible (a possible probe of an eld PTP base), all strategies to obtain PTP's (reter/passed and /rete/group likes, and a list of all list storage in the path observes). The produce to the path observes are assessed for an end housing for account more to try, and passwerd fairs ret housing for account produces are adapted with the path observes. The produce the path observes are adapted by the produce the storage and the path observes are adapted by the path observes and the path obser

 Televelogie: All logis attempts are logged and reviewed daily. It is easy to spot when somecore is trying many account, or harmening on a particular account. Since there are no authorized accounts for Internet users on our gateway: other than sparaft, it is easy to pick our problem.

Guardiniser account: A public computer account in the first thing a cracker looks for. These accounts provide friendly, easy accounts to easily every file is the machine, including the password lile. The unskire can also get a line of boots to do the second by this machine from the /eter/how to .equiv and various personal , zhowtas files. Our login script for these accounts low something like this:

ENHANCING COMPUTER SYSTEM SECURITY Dennis Hollingworth

August 1973

P-5064

Information Decoys

- Existing work on use of decoys ("honeytokens")
 - Large scale
 - Automated generation and management
 - Ubiquitous/pervasive

Why?

Focus on attack target: information
 It will leak



Attempt to sidestep the technical arms race

Decoys as a Primitive

- Decoys/deception should be considered a general purpose primitive in cybersecurity, akin to cryptography
- Properties
 - diverse
 - flexible
 - principled
 - measurable

Decoy Properties

- Believability
- Enticingness
- Detectability
- Variability
- Conspicuousness
- Non-interference



Believability Formalization

- Defined for object space M and decoy set D
- Decoy Believability Experiment
 - For any $d \in D$, choose two objects $m_0, m_1 \in M$ such that $m_0 = d$ or $m_1 = d$, and $m_0 \neq m_1$
 - Adversary A obtains m_0 , m_1 and attempts to choose $m^* \in \{m_0, m_1\}$ such that $m^* != d$, using only information intrinsic to m_0 , m_1
 - The output of the experiment is 1 if m* != d and 0 otherwise.
- Perfect decoy when: Pr[Exp_{believe}=1]=1/2

Broad Applications

- Network eavesdropping [WiSec 2009]
- Tor eavesdropping [RAID 2011]
- Keystroke loggers/rootkits [RAID 2010]
- Source code [ASIACCS 2012]
- Documents (unstructured data) [SecureComm 2009]

Computational Decoys

- Move from data to computation
 Not entirely distinct
- Create uncertainty and confusion to adversaries that gain access to the cloud infrastructure

Computational Decoys: Goal

- Make it impossible to determine whether a captured system is handling real or decoy processing within N time units
 - Time units are envisioned to be in the order of hours or days

 Opportunity for detection, misdirection, and <u>engagement with adversary</u>

Assumptions

- Partitioned, replicated applications (cloud!)
- Adversary can have access to full system
 Possibly including root/kernel-level access
- Adversary cannot see all network traffic inside and into/out of the cloud
 - Adversary cannot determine whether a specific connection is from the outside or from a cloud-local proxy, except for adversary's own connections
- Adversary cannot readily determine ground truth in most cases

PoC: DIGIT

- Goal: create uncertainly to the adversary as to what is real
- Threat model: unknown number of replicas is compromised
 - Compromised replicas receive requests with mission-sensitive info
 - Adversary does not control user input or issue requests



Application-level Traffic Interceptor

- TLS terminator and incoming network traffic inspector
- Application-level protocol Identifier
 - Currently: port-based (e.g., 80 is HTTP) and single-message protocol-based (e.g., filters matching HTTP requests)
- Application-specific user input parsing (modules)
 - pairs incoming user-initiated requests with similar decoy requests to produce a legitimate-decoy traffic mix
 - decoys are generated offline and stored in the decoy store
 - randomly disseminates the legitimate-decoy traffic mix to the set of replicas, designated to handle original client request
 - reconciles replies from replicas and forwards the result to answer client's request

- Generate input variations for client's request
 - Context-aware application input randomization
 - Example case: Web applications
 - Interaction endpoints with clients are well-defined and documented
 - Application-specific modules are written to identify the variable parts of incoming requests and invoke appropriate randomization routine (e.g., byte-range or dictionary based)
 - Are these variations plausible?



- Identify variations exhibiting similar application behavior
 - 1. Evaluate application behavior for generated decoys
 - Dynamic binary instrumentation of (Web) application with a PIN tool
 - Output of application execution decisions (CFG, BB, SysCalls)



- Identify variations exhibiting similar application behavior
 - 2. Similarity grouping based on application execution path
 - Execution trace evaluation tool determines alignment of decoy-input behavior with actual-input behavior.
 - Strict mode: absolute or near-absolute alignment
 - Relaxed mode: deviations are permitted as long as both traces align at the beginning and end and overlap more than T %.



- Identify variations exhibiting similar application behavior
 - 2. Similarity grouping based on application execution path
 - Evaluated on simple custom-built Web applications.
 - Aligned successfully different HTTP or application-level responses (HTTP errors, valid HTTP response and in-app error message) with execution trace deviations. Input variations included URL fuzzing and HTTP header manipulation.
- Production of decoy-traffic groups, indexed by legitimate traffic template, stored in decoy traffic database
- Used in real-time by application-level traffic interceptor

Reachback

- Decoy computation as cover traffic for payloads
 - Active information gathering
 - Forensic analysis (CI)
 - Other payloads...

	mo/alertsdetails.html			☆ ⊽ C	Ightning talks shmoocor
Custom Policy	y Name 3 minutos ago 11/21/	2011 16:46 dc748o628aco0ca9111bco7	Rica78c37 Close		
Policy Violation	Data Aquisition Vessel Hist	ary .			
Policy	Trigger		Actual		
Custom Policy Name	IP Address is outside range: 123.123.12	3 0 - 123 123 123 266	567.687.567		
Actions Taken:	Variable Value	Time of Execution ID			
Alert Generated	For Mo	11/21/2011 15:45 69/45057±5063	28e62561a13dc9bccs7		
Alert Generated	Fer Group XYZ	11/21/2011 15:45 92h10f7cTeceff	77415De91152Eu9488		
Ernal Sent	to abo123@mycompany.com	11/21/2011 15:45 dbab9/71ccc49	5127/d06407a68bde104		
ana Bill	to droup XYZ	11/21/2011 10:40 425840202260 11/21/2011 16:46 3331-0487-048	10/00243034820131		
Water of the second second second	 - Jo vessel Security Score - New Score 90 key AcOM/LIGHD/RMD/RMM/2015/77/77-1474 	11/21/2011 15:45 35eff15efc1070	01009409021048ed7		
Vessel self encrypt	key: 261cd90s540c07e077e00s882e1e34e	11/21/2011 15:45 b9/45057:50b3	28x6296tx12dc8bccv7		
Germany Autor Italy Greece	Ukraine Address: 1110 Budspest, Telephone +36 (1) 371-031 Telephone +36 (1) 371-031 Telephone +36 (1) 371-032 Homegage wew threade bu Turn facebook: www.facebook.com/	Kondorfa u. 6.			
Active Rom Italy Creece Asset History Unit	Adverse Adverse Herein	Gostra u. 8. Melcostra semane	angur 1		

Challenges/Next Steps

- Scenario construction
- Characterize supported application (and data) complexity
 - -e.g., use of crypto at the application layer
 - Can we <u>design</u> applications/systems with computation decoys in mind?
- Resource expenditure
 - Fine-grained I/O multiplexing across replicas
- Evaluation/validation