Forecasting Malware Capabilities From Cyber Attack Memory Images

Omar Alrawi*, Moses Ike*, Matthew Pruett, Ranjita Pai Kasturi, Srimanta Barua, Taleb Hirani, Brennan Hill, and Brendan Saltaformaggio

*First Co-Authors
Motivating Example: DarkHotel APT
Motivating Example: DarkHotel APT

Spear Phishing Email

- DarkHotel Operator
- CEO's Computer
Motivating Example: DarkHotel APT
Motivating Example: DarkHotel APT
Motivating Example: DarkHotel APT
Motivating Example: DarkHotel APT
Motivating Example: DarkHotel APT
Motivating Example: DarkHotel APT

DarkHotel Operator

CEOs Computer
Motivating Example: DarkHotel APT

Jim, Incident Responder

DarkHotel Operator

CEO’s Computer

Potentially harmful software detected
Click to review and take action
Motivating Example: DarkHotel APT

Jim, Incident Responder

DarkHotel Operator

CEO's Computer
Motivating Example: DarkHotel APT

Jim, Incident Responder

Goal: Jim must get ahead of the attacker
Motivating Example: DarkHotel APT

Jim, Incident Responder

Goal: Jim must get ahead of the attacker

Jim must assess the extent of the breach
Motivating Example: DarkHotel APT

Jim, Incident Responder

Goal: Jim must get ahead of the attacker

Jim must assess the extent of the breach

DarkHotel Operator

CEO's Computer
Motivating Example: DarkHotel APT

Jim, Incident Responder

Goal: Jim must get ahead of the attacker

Jim must assess the extent of the breach
Motivating Example: DarkHotel APT

Jim, Incident Responder

Goal: Jim must get ahead of the attacker

Jim must assess the extent of the breach

Jim must proactively deploy defenses for upcoming payloads
Incident Response Process

Malware

Challenges
Challenge

- Manual analysis is slow and requires context switching
- Prone to human errors
Incident Response Process

Challenges
- Manual analysis is slow and requires context switching
- Prone to human errors
- C&C server is down (malware refuses to run)
- Anti-analysis techniques
Incident Response Process

Challenges

- Manual analysis is slow and requires context switching
- Prone to human errors
- C&C server is down (malware refuses to run)
- Anti-analysis techniques
- Heuristic signatures have false-negatives (miss important artifacts)

Malware
Static Analysis
Volatility Memory Analysis
Malware Sandbox Analysis
C&C
Let’s Help Jim

All Jim needs is the malware memory image
Let’s Help Jim

All Jim needs is the malware memory image
Let’s Help Jim

All Jim needs is the malware memory image
Let’s Help Jim

Data Structure

Key Idea: Reanimate the Malware’s State

Code Segments

```assembly
push    ebp
mov     ebp, esp
movzx   ecx, [ebp+arg_0]
pop     ebp
movzx   dx, cl
lea     eax, [edx+edx]
add     eax, edx
shl     eax, 2
add     eax, edx
shr     eax, 8
sub     cl, al
shr     cl, 1
add     al, cl
shr     al, 5
movzx   eax, al
```
Let's Help Jim

Key Idea: Reanimate the Malware's State

Data Structure

Code Segments

Symbolic Analysis

push ebp
mov ebp, esp
movzx ecx, [ebp+arg_0]
pop ebp
movzx dx, cl
lea eax, [edx+edx]
add eax, edx
shl eax, 2
add eax, edx
shr eax, 8
sub cl, al
shr cl, 1
add al, cl
shr al, 5
movzx eax, al
retn
Let’s Help Jim

Data Structure

Key Idea: Reanimate the Malware’s State

Symbolic Analysis
Let’s Help Jim

C&C Domain: mse.vmmnat.com

Data Structure

Key Idea: Reanimate the Malware’s State

Symbolic Analysis

Code Segments

```
push ebp
mov ebp, esp
mov ecx, [ebp+arg_0]
pop ebp
mov ecx, cl
lea edx, [edx+ecx]
add eax, edx
shl eax, 2
add eax, edx
shr eax, 9
sub al, eax
shr cl, 1
add al, cl
shr al, 5
movzx eax, al
ret
```
Let's Help Jim

Data Structure

Code Segments

C&C Domain: mse.vmmnat.com

Key Idea: Reanimate the Malware’s State

Incident Responder’s Goal:
Automatically Identify and Forecast Stagged Capabilities

Probability of C&C Connection 54%
Probability of Code Injection 31%
Probability of File Exfiltration 15%
FORECAST

Malware Memory Dump

Context-Aware Memory Forensics
Malware Memory Dump

Parser

Memory Image

Execution Context

Context-Aware Memory Forensics

FORECAST
Malware Memory Dump

Memory Image Concrete
Execution Context

Context-Aware Memory Forensics
Malware Memory Dump

Memory Image Concrete
Execution Context

Parser

Context-Aware Memory Forensics

Augmented Symbolic Exploration
Probability Assignment
Capability-Relevant Paths

Probabilistic Symbolic Analysis

FORECAST
Malware Memory Dump

Context-Aware Memory Forensics

Memory Image Concrete Execution Context

Augmented Symbolic Exploration Probability Assignment Capability-Relevant Paths

Probabilistic Symbolic Analysis
Malware Memory Dump

Malware Memory Dump

Memory Image Concrete

Execution Context

Forward Explore Staged Malware Capabilities

Augmented Symbolic Exploration

Probability Assignment

Capability-Relevant Paths

Context-Aware Memory Forensics

Probabilistic Symbolic Analysis

FORECAST
Symbolic and Concrete Mixing

- Quantify the mixing of symbolic and concrete values
- Analogous to weather forecasting (cloud, humidity, etc.)
Symbolic and Concrete Mixing

- Quantify the mixing of symbolic and concrete values
- Analogous to weather forecasting (cloud, humidity, etc.)
- Put Simply:
  - Paths that access more concrete state are staged to execute soon
  - Paths that access more symbolic state are less likely to execute
Augmented Symbolic Exploration
Probability Assignment
Capability-Relevant Paths

Context-Aware Memory Forensics
Probabilistic Symbolic Analysis

FORECAST

Malware Memory Dump

Parse Memory Image
Recover Execution Context

Forward Explore Stagged Malware Capabilities

Memory Image
Parser
CODE
DATA
EAX, EBX, ECX, EDX, EIP, ESP, ESI, EDI, EFLAGS

Execution Context
Parse Memory Image  
Recover Execution Context  
Forward Explore Staged Malware Capabilities

Malware Memory Dump

Augmented Symbolic Exploration  
Probability Assignment  
Capability-Relevant Paths

Context-Aware Memory Forensics  
Probabilistic Symbolic Analysis

Capability Plugin Analysis  
Capability Forecast

31% Code Injection  
15% File Exfiltration  
54% C&C URL
Malware Memory Dump

Parse Memory Image
Recover Execution Context

Forward Explore Staged Malware Capabilities

Exfiltration
Code Injection
C&C Comm.

Augmented Symbolic Exploration
Probability Assignment
Capability-Relevant Paths

Probabilistic Symbolic Analysis

Context-Aware Memory Forensics

Parser
Memory Image
Execution Context

FORECAST

Malware Memory Dump

Code Injection 31%
File Exfiltration 15%
C&C URL 54%

Capability Forecast

Capability Plugin Analysis
Evaluation Setup

6,727 Malware Samples
274 Families

FORECAST
Evaluation Setup

6,727 Malware Samples
274 Families

FORECAST
Evaluation Setup

6,727 Malware Samples
274 Families

FORECAST

C&C Domain: mse.vmmnat.com
Evaluation Setup

6,727 Malware Samples
274 Families

FORECAST

IDS Alert

C&C Domain:
mse.vmmnat.com
Evaluation Setup

6,727 Malware Samples
274 Families

IDS Alert
C&C Domain: mse.vmmnat.com
Evaluation Setup

- 6,727 Malware Samples
- 274 Families

Evaluation Highlights

- Average accuracy of 95% on manual reverse engineered malware
- Average exploration time 291 seconds
- Average of 26 APIs and 1,638 states per exploration task
- Dropper and Persistence in 70% of samples

C&C Domain: mse.vmmnat.com
# Ground Truth Deep Dive

<table>
<thead>
<tr>
<th>Malware</th>
<th>C&amp;C Comm</th>
<th>File Exfiltration</th>
<th>Code Injection</th>
<th>Dropper</th>
<th>Key &amp; Screen Spy</th>
<th>Persistence</th>
<th>Anti-analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$P_F$ $O_M$ $O_F$</td>
<td>$P_F$ $O_M$ $O_F$</td>
<td>$P_F$ $O_M$ $O_F$</td>
<td>$P_F$ $O_M$ $O_F$</td>
<td>$P_F$ $O_M$ $O_F$</td>
<td>$P_F$ $O_M$ $O_F$</td>
<td>$O_{FP}$ $O_{FN}$</td>
</tr>
<tr>
<td>Bokbok</td>
<td>38% 2 2</td>
<td>5% 3 3</td>
<td>57% 1 1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0 0</td>
</tr>
<tr>
<td>AcridRain</td>
<td>23% 3 3</td>
<td>19% 4 4</td>
<td>-</td>
<td>28% 2 2</td>
<td>-</td>
<td>30% 1 1</td>
<td>0 0</td>
</tr>
<tr>
<td>AthenaGo</td>
<td>- 11% 4 4</td>
<td>- 22% 3 2</td>
<td>-</td>
<td>-</td>
<td>33% 2 3</td>
<td>34% 1 1</td>
<td>2 0</td>
</tr>
<tr>
<td>Rokrat</td>
<td>30% 1 1</td>
<td>26% 2 2</td>
<td>22% 3 3</td>
<td>-</td>
<td>17% 4 4</td>
<td>-</td>
<td>15% 5 5</td>
</tr>
<tr>
<td>AdamLocker</td>
<td>22% 3 3</td>
<td>0 4 0</td>
<td>45% 1 1</td>
<td>-</td>
<td>-</td>
<td>33% 2 2</td>
<td>0 1</td>
</tr>
<tr>
<td>Marap</td>
<td>- 46% 3 3</td>
<td>- 40% 1 1</td>
<td>-</td>
<td>14% 2 2</td>
<td>-</td>
<td>-</td>
<td>0 0</td>
</tr>
<tr>
<td>ATI</td>
<td>-</td>
<td>-</td>
<td></td>
<td>41% 2 2</td>
<td>-</td>
<td>42% 1 1</td>
<td>17% 3 3</td>
</tr>
<tr>
<td>TeslaAgent</td>
<td>11% 4 4</td>
<td>14% 3 3</td>
<td>32% 1 1</td>
<td>-</td>
<td>13% 2 3</td>
<td>30% 3 3</td>
<td>0 0</td>
</tr>
<tr>
<td>Andromeda</td>
<td>25% 2 2</td>
<td>- 14% 3 3</td>
<td>-</td>
<td>-</td>
<td>61% 1 1</td>
<td>-</td>
<td>0 0</td>
</tr>
<tr>
<td>AveMaria</td>
<td>28% 3 4</td>
<td>29% 2 2</td>
<td>28% 4 3</td>
<td>-</td>
<td>25% 1 1</td>
<td>0 3 0</td>
<td>2 1</td>
</tr>
<tr>
<td>Aveo</td>
<td>22% 3 3</td>
<td>-</td>
<td>-</td>
<td>40% 1 1</td>
<td>-</td>
<td>38% 2 2</td>
<td>0 4 0</td>
</tr>
<tr>
<td>7Honest</td>
<td>- 16% 3 3</td>
<td>- 51% 1 1</td>
<td>-</td>
<td>-</td>
<td>11% 4 4</td>
<td>-</td>
<td>22% 2 2</td>
</tr>
<tr>
<td>Abaddon</td>
<td>- 26% 2 2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>84% 1 1</td>
<td>0 0</td>
</tr>
<tr>
<td>AVCrypt</td>
<td>51% 1 1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>19% 3 3</td>
<td>30% 2 2</td>
</tr>
</tbody>
</table>

Table 1: Capability Forecasts of 14 Select Recent Samples. $P_F$: Forecast percentage, $O_M$: Ground truth manual ordering, $O_F$: FORECAST ordering, $O_{FP}$: Ordering false positive, $O_{FN}$: Ordering false negative.
## Ground Truth Deep Dive

<table>
<thead>
<tr>
<th>Malware</th>
<th>C&amp;C Comm Exfiltration</th>
<th>File Exfiltration</th>
<th>Code Injection</th>
<th>Dropper</th>
<th>Key &amp; Screen Spy</th>
<th>Persistence</th>
<th>Anti-analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(P_F)</td>
<td>(O_M)</td>
<td>(O_F)</td>
<td>(P_F)</td>
<td>(O_M)</td>
<td>(O_F)</td>
<td>(P_F)</td>
</tr>
<tr>
<td>Bokbok</td>
<td>38%</td>
<td>2</td>
<td>2</td>
<td>5%</td>
<td>3</td>
<td>3</td>
<td>57%</td>
</tr>
<tr>
<td>AcridRain</td>
<td>23%</td>
<td>3</td>
<td>3</td>
<td>19%</td>
<td>4</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>AthenaGo</td>
<td>-</td>
<td>4%</td>
<td>4</td>
<td>-</td>
<td>11%</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>Rokrat</td>
<td>30%</td>
<td>1</td>
<td>1</td>
<td>26%</td>
<td>2</td>
<td>2</td>
<td>22%</td>
</tr>
<tr>
<td>AdamLocke</td>
<td>22%</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>4%</td>
<td>0</td>
<td>45%</td>
</tr>
<tr>
<td>Marap</td>
<td>-</td>
<td>46%</td>
<td>3</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>40%</td>
</tr>
<tr>
<td>ATI</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>41%</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>TeslaAgent</td>
<td>11%</td>
<td>4</td>
<td>4</td>
<td>14%</td>
<td>3</td>
<td>3</td>
<td>32%</td>
</tr>
<tr>
<td>Andromeda</td>
<td>25%</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>14%</td>
<td>3</td>
</tr>
<tr>
<td>AveMaria</td>
<td>28%</td>
<td>3</td>
<td>4</td>
<td>29%</td>
<td>2</td>
<td>2</td>
<td>28%</td>
</tr>
<tr>
<td>Aveo</td>
<td>22%</td>
<td>3</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>40%</td>
<td>1</td>
</tr>
<tr>
<td>7Honest</td>
<td>-</td>
<td>16%</td>
<td>3</td>
<td>3</td>
<td>51%</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Abaddon</td>
<td>-</td>
<td>26%</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>AVCrypt</td>
<td>51%</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

|\(O_{FP}\) | | | \(O_{FN}\)|
|------------|------------|------------|
| 0          | 0          | 0          |

Table 1: Capability Forecasts of 14 Select Recent Samples. \(P_F\): Forecast percentage, \(O_M\): Ground truth manual ordering, \(O_F\): FORECAST ordering, \(O_{FP}\): Ordering false positive, \(O_{FN}\): Ordering false negative.
# Ground Truth Deep Dive

## 14 Malware Families

![Security Reports](image1.png) ![Reverse Engineer](image2.png)

<table>
<thead>
<tr>
<th>Malware</th>
<th>XC Comm</th>
<th>File Exfiltration</th>
<th>Code Injection</th>
<th>Dropper</th>
<th>Key &amp; Screen Spy</th>
<th>Persistence</th>
<th>Anti-analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$P_F$</td>
<td>$O_M$</td>
<td>$O_F$</td>
<td>$P_F$</td>
<td>$O_M$</td>
<td>$O_F$</td>
<td>$P_F$</td>
</tr>
<tr>
<td>Bokbok</td>
<td>38%</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>AcrinRain</td>
<td>23%</td>
<td>3</td>
<td>3</td>
<td>-</td>
<td>28%</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>AthenaGo</td>
<td>-</td>
<td>11%</td>
<td>4</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>33%</td>
</tr>
<tr>
<td>Rokrat</td>
<td>30%</td>
<td>1</td>
<td>1</td>
<td>26%</td>
<td>22%</td>
<td>3</td>
<td>34%</td>
</tr>
<tr>
<td>AdamLocker</td>
<td>22%</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>45%</td>
<td>1</td>
<td>15%</td>
</tr>
<tr>
<td>Marap</td>
<td>-</td>
<td>46%</td>
<td>3</td>
<td>4</td>
<td>40%</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>ATI</td>
<td>-</td>
<td>-</td>
<td>41%</td>
<td>2</td>
<td>-</td>
<td>14%</td>
<td>0</td>
</tr>
<tr>
<td>TeslaAgent</td>
<td>11%</td>
<td>4</td>
<td>3</td>
<td>14%</td>
<td>32%</td>
<td>1</td>
<td>17%</td>
</tr>
<tr>
<td>Andromeda</td>
<td>25%</td>
<td>2</td>
<td>2</td>
<td>29%</td>
<td>14%</td>
<td>3</td>
<td>30%</td>
</tr>
<tr>
<td>AveMaria</td>
<td>28%</td>
<td>3</td>
<td>2</td>
<td>29%</td>
<td>28%</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Aveo</td>
<td>22%</td>
<td>3</td>
<td>3</td>
<td>-</td>
<td>40%</td>
<td>1</td>
<td>38%</td>
</tr>
<tr>
<td>7Honest</td>
<td>-</td>
<td>16%</td>
<td>3</td>
<td>51%</td>
<td>11%</td>
<td>4</td>
<td>22%</td>
</tr>
<tr>
<td>Abaddon</td>
<td>-</td>
<td>26%</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>84%</td>
<td>2</td>
</tr>
<tr>
<td>AVCrypt</td>
<td>51%</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>19%</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 1: Capability Forecasts of 14 Select Recent Samples. $P_F$: Forecast percentage, $O_M$: Ground truth manual ordering, $O_F$: FORECAST ordering, $O_{FP}$: Ordering false positive, $O_{FN}$: Ordering false negative.
Read The Full Paper:
Forecasting Malware Capabilities From Cyber Attack Memory Images.
Omar Alrawi*, Moses Ike*, Matthew Pruett, Ranjita Pai Kasturi,
Srimanta Barua, Taleb Hirani, Brennan Hill, Brendan Saltaformaggio

Code: https://github.com/CyFI-Lab-Public/Forecast

Thank you! Questions?

Omar Alrawi
alrawi@gatech.edu
https://alrawi.io