Indicators of Compromise

draft-paine-smart-indicators-of-compromise

Ollie Whitehouse, NCC Group

History

• Available on Datatracker:

<u>https://tools.ietf.org/html/draft-paine-smart-indicators-of-compromis</u> <u>e-03</u>

- Presented -00 at secdispatch in IETF 109
- Revised based on feedback on list and in meeting
- Brought to OPSEC mailing list this year
- Thanks to Nancy Camwinget and Fernando Gont for their thorough reviews on -02

Motivation

- To document this existing operational security practice as a baseline
- To share knowledge with protocol engineers on a commonly used technique in cyber defence
- To prevent this technique being accidentally ignored
 - Engineers can make protocol design choices that affect IoC availability
 - So we'd like the IETF community at large to know about IoC techniques
- To bring cyber defence expertise into the IETF and share it through an Informational RFC, and begin cross-pollination of industry experiences

Draft introduction

Indicators of Compromise (IoCs) and Their Role in Attack Defence draft-paine-smart-indicators-of-compromise-03

Abstract

Cyber defenders frequently rely on Indicators of Compromise (IoCs) to identify, trace, and block malicious activity in networks or on endpoints. This draft reviews the fundamentals, opportunities, operational limitations, and best practices of IoC use. It highlights the need for IoCs to be detectable in implementations of Internet protocols, tools, and technologies - both for the IoCs' initial discovery and their use in detection - and provides a foundation for new approaches to operational challenges in network security.

Draft structure

Old

<u>1</u> . Introduction	<u>2</u>
<u>1.1</u> . Requirements Language	3
2. Terminology	3
3. What are IoCs?	3
- 4. Why use IoCs?	4
4.1. ToCs can be used even with limited resource	4
4.2 To(s have a multiplier effect on attack defence effort	5
4.2. Tols and oscily shaneable	5
$\frac{4.5}{100}$	2
4.4. Toos can be attributed to specific threat actors	2
4.5. Tols can provide significant time savings	<u>6</u>
<u>4.6</u> . IoCs allow for discovery of historic attacks	<u>6</u>
4.7. IoCs underpin and enable multiple layers of the modern	
defence-in-depth strategy	<u>6</u>
5. Pain, Fragility and Precision	Z
<u>5.1</u> . Pyramid of Pain	7
5.2. Fragility	9
5.3. Precision	9
5.4. Comprehensive Coverage	9
6. Defence in Depth	10
7. Case Study: APT33	12
7.1 Ovenall TTP	12
$\frac{7.1}{7.2}$	12
$\frac{1}{2}$	13
<u>8</u> . Conclusions	13

New

1.1. Requirements Language 3 2. Terminology 3 3. IOC Fundamentals 4 3.1. IOC Types and the Pyramid of Pain 4 3.2. IOC Lifecycle 8 3.2.1. Discovery 8 3.2.2. Assessment 8 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 10 3.2.7. End of Life 10 4.1.1. Oportunities 10 4.1.2. IoCs can be used even with limited resources 11 4.1.2. IoCs are easily shared 13 4.1.3. IoCs are easily shared 13 4.1.4. IoCs are be attributed to specific threats 14 4.2. Case Studies 13 4.1.2. IoV and be attributed to specific threats 14 4.2.2.2. IoV and the attributed to specific threats 14 <th>1.</th> <th>Introduc</th> <th>tion</th> <th></th> <th></th> <th></th> <th>3</th>	1.	Introduc	tion				3
2. Terminology 3 3. ICC Fundamentals 4 3.1. ICC Types and the Pyramid of Pain 4 3.2. ICC Lifecycle 8 3.2.1. Discovery 8 3.2.2. Assessment 9 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 10 3.2.6. Reaction 10 3.2.7. End of Life 10 4.1.0 Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.2. Cobalt Strike 14 4.2.3.1. Overall TTP 15 4.2.3.1. Overall TTP 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 15 4.2.3.3. APT33 15	1	.1. Requ	uirements Language				3
3. IOC Fundamentals 4 3.1. IOC Types and the Pyramid of Pain 4 3.2. IOC Lifecycle 8 3.2.1. Discovery 8 3.2.2. Assessment 8 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 10 3.2.7. End of Life 10 3.2.7. End of Life 10 3.2.7. End of Life 10 4.1. Opportunities 10 4.1. Opportunities 10 4.1. IoCs can be used even with limited resources 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs and provide significant time savings 13 4.1.4. IoCs and provide significant time savings 13 4.1.5. IoCs can provide significant time savings 14 4.2.1. Introduction 14 4.2.2.1. Introduction 14 4.2.2.2. IoCs IoCs 4.2.3.1. Overall TTP <td< td=""><td>2.</td><td>Terminol</td><td>Logv</td><td></td><td></td><td></td><td>3</td></td<>	2.	Terminol	Logv				3
3.1. IoC Types and the Pyramid of Pain 4 3.2. IoC Lifecycle 8 3.2.1. Discovery 8 3.2.2. Assessment 8 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 10 3.2.6. Reaction 10 3.2.7. End of Life 10 4.1. Opportunities 10 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 13 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.2.1. Introduction 14 4.2.2.2. IoCs 15 4.2.3.1. Overall TTP 15 4.2.4.1. Overall TTP 16 4.2.2.2.1 IoCs 16 4.2.3.2.1 Cocs 17 5.1.1.1. Fragility 17	3.	IoC Fund	Jamentals				4
3.2. IoC Lifecycle 8 3.2.1. Discovery 8 3.2.2. Assessment 8 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 10 3.2.6. Reaction 10 3.2.7. End of Life 10 4.1. Opportunities 10 4.1. Opportunities 11 4.1.1. IOCs underpin and enable multiple layers of the modern defence in depth strategy 11 4.1.2. IOCs can be used even with limited resources 11 4.1.3. IOCs are easily shared 13 4.1.4. IOCs are easily shared 13 4.1.5. IOCs can be attributed to specific threats 14 4.1.7. IOCs can be attributed to specific threats 14 4.2.2. Cobalt Strike 14 4.2.2.1. Introduction 14 4.2.2.2. IOCs 15 4.2.3.1. Overall TTP 15 4.2.3.2. IOCs 16 4.2.3.3. IOCs	3	1. IoC	Types and the Pyramid of Pain				4
3.2.1. Discovery 8 3.2.2. Assessment 8 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 10 3.2.7. End of Life 10 3.2.7. End of Life 10 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can be attributed to specific threats 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.2. Cobalt Strike 14 4.2.2. Cobalt Strike 14 4.2.2. IoCs 15 4.2.3. APT33 15 4.2.3. APT33 15 4.2.3. Precision 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 </td <td>3</td> <td>.2. IoC</td> <td>Lifecvcle</td> <td></td> <td></td> <td></td> <td>8</td>	3	.2. IoC	Lifecvcle				8
3.2.2. Assessment 8 3.2.3. Sharing 9 3.2.4. Deployment 9 3.2.5. Detection 9 3.2.6. Reaction 10 3.2.7. End of Life 10 4. Using IoCs Effectively 10 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can be displicant time savings 13 4.1.6. IoCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 15 4.2.3.2. IoCs 16 4.2.3.2. IoCs 16 4.2.3.2.	_	3.2.1.	Discovery		Ì		8
3.2.3. Sharing		3.2.2.	Assessment		÷		8
3.2.4. Deployment 9 3.2.5. Detection 10 3.2.7. End of Life 10 4.1. Using IoCs Effectively 10 4.1. Opportunities 10 4.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.7. IoCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2.1. Overall TTP 15 4.2.3.1. Overall TTP 15 4.2.3.1. Overall TTP 16 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 17 5.1.1. Fragility 17 5.1.2. Deciricity		3 2 3	Sharing	•	•	•	g
3.2.5. Detection 10 3.2.6. Reaction 10 3.2.6. Reaction 10 4. Using IoCs Effectively 10 4.1. Opportunities 10 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.1 Introduction 14 4.2.2.1 Overall TTP 15 4.2.2.1 Overall TTP 15 4.2.3.1 Overall TTP 16 4.2.3.1 Overall TTP 16 4.2.3.2 IoCs 17 5.1.1 Fragility 17 5.1.2. Discoverability 18 <		3 2 4	Denloyment	•	•	•	2 Q
3.2.6. Reaction 10 3.2.7. End of Life 10 4. Using IoCs Effectively 10 4.1. Opportunities 10 4.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.1. IoCs can be used even with limited resources 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.1 Introduction 14 4.2.2. Cobalt Strike 15 4.2.2.1. Overall TTP 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 17 5.1.1. Fragility 17 5.1.1. Fragility 17 5.1.1. Fragility 19 5.2.2.		3 2 5		•	•	•	10
3.2.7. End of Life 10 4. Using IoCs Effectively 10 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs can be used even with limited resources 11 4.1.4. IoCs are easily shared 12 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.2. Cose Studies 14 4.2.2. Cose Studies 14 4.2.2. Cose Studies 14 4.2.2. IoCs 15 4.2.2.1. Introduction 14 4.2.2.2. IoCs 15 4.2.3.1. Overall TTP 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5.2.0perational Limitations 17 5.1.1. Fragility 17		22.5.		•	•	•	10
4. Using IoCs Effectively 10 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.2. Cobalt Strike 14 4.2.2.1. Introduction 14 4.2.2.2. IoCs 15 4.2.3.1 Overall TTP 15 4.2.3.2 IoCs 15 4.2.3.2 IoCs 16 5.0 Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2.1. Specificity 19 5.2.1. Specificity 19 5.3. Privacy 20 5.4. Automation 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		$\frac{5.2.0}{2.2.7}$	End of Life	•	•	•	10
4. Osing loss Prietrively 1 4.1. Opportunities 10 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.2. Cobalt Strike 14 4.2.2.2. IoCs 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21	4	<u>3.2.7</u> .	C. Effectively	•	•	•	10
4.1. Opportunities 1 4.1.1. IoCs underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs can be used even with limited resources 11 4.1.4. IoCs are easily shared 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 17 5.1.1. Fragility 17 5.1.2. Discoverability 17 5.1.3. Specificity 19 5.2. Precision 19 5.2.1. Specificity 19	±.			•	•	•	10
4.1.1. locs Underpin and enable multiple layers of the modern defence-in-depth strategy 11 4.1.2. locs can be used even with limited resources 11 4.1.3. locs have a multiplier effect on attack defence effort 12 4.1.4. locs are easily shared 13 4.1.5. locs can provide significant time savings 13 4.1.6. locs can provide significant time savings 13 4.1.7. locs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. locs 15 4.2.3.1. Overall TTP 16 4.2.3.2. locs 16 4.2.3.2. locs 17 5.1.1. Fragility 17 5.1.2. Discoverability 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use	4	<u>. </u>		•	•	•	10
modern defence-in-depth strategy 11 4.1.2. IoCs can be used even with limited resources 11 4.1.3. IoCs have a multiplier effect on attack defence effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.6. IoCs allow for discovery of historic attacks 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3.1. Overall TTP 15 4.2.3.2. IoCs 15 4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.1. Specif		4.1.1.	locs underpin and enable multiple layers of the				
4.1.2. locs can be used even with limited resources 11 4.1.3. locs have a multiplier effect on attack defence effort 12 4.1.4. locs are easily shared 13 4.1.5. locs can provide significant time savings 13 4.1.6. locs can be attributed to specific threats 13 4.1.7. locs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2.1. Introduction 14 4.2.2.2. cobalt Strike 14 4.2.2.2. locs 15 4.2.2.2. locs 15 4.2.3.1 Overall TTP 15 4.2.3.2. locs 15 4.2.3.1. Overall TTP 16 4.2.3.2. locs 17 5.1.1 Fragility 17 5.1.2. Discoverability 17 5.1.2. Discoverability 19 5.2.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compro			modern defence-in-depth strategy	•	•	•	<u>11</u>
4.1.3. Locs have a multiplier effect on attack defence effort		<u>4.1.2</u> .	locs can be used even with limited resources .	•	•	•	<u>11</u>
effort 12 4.1.4. IoCs are easily shared 13 4.1.5. IoCs can provide significant time savings 13 4.1.6. IoCs allow for discovery of historic attacks 13 4.1.7. IoCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5.0 Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 17 5.1.2. Discoverability 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21		4.1.3.	locs have a multiplier effect on attack defence				
4.1.4. IOCs are easily shared 13 4.1.5. IOCs can provide significant time savings 13 4.1.6. IOCs allow for discovery of historic attacks 13 4.1.7. IOCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 14 4.2.2.2. IoCs 15 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 4.2.3.2. IoCs 16 5.0 Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Au			effort	•	•	•	<u>12</u>
4.1.5. IOCs can provide significant time savings 13 4.1.6. IOCs allow for discovery of historic attacks 13 4.1.7. IOCs can be attributed to specific threats 14 4.2.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2. IoCs 15 4.2.3. IoCs 15 4.2.3. IoCs 15 4.2.3.1 Overall TTP 16 5.1 Time and Effort 17 5.1.1 Fragility 17 5.1.2. Discoverability 18 5.2. Preci		4.1.4.	IoCs are easily shared	•	•	•	<u>13</u>
4.1.6. IOCs allow for discovery of historic attacks 13 4.1.7. IOCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 15 4.2.3.1 Overall TTP 15 4.2.3.1 Overall TTP 16 5.0 Operational Limitations 17 5.1.1 Fragility 17 5.1.2. Discoverability 17 5.1.2. Discoverability 19 5.2.1. <		4.1.5.	IoCs can provide significant time savings	•	•	•	<u>13</u>
4.1.7. IoCs can be attributed to specific threats 14 4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 14 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5.0 Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		4.1.6.	IoCs allow for discovery of historic attacks .	•	•	•	<u>13</u>
4.2. Case Studies 14 4.2.1. Introduction 14 4.2.2.1. Observation 14 4.2.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3. Ioverall TTP 16 4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21		4.1.7.	IoCs can be attributed to specific threats	•	•	•	<u>14</u>
4.2.1. Introduction 14 4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6.1. Comprehensive Coverage and Defence-in-Depth 21	<u>4</u>	<u>.2</u> . Case	9 Studies	•	•	•	<u>14</u>
4.2.2. Cobalt Strike 14 4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3.1 Overall TTP 15 4.2.3.1 Overall TTP 16 4.2.3.2 IoCs 16 5. Operational Limitations 17 5.1.1 Fragility 17 5.1.2 Discoverability 18 5.2. Precision 19 5.2.2 Dual and Compromised Use 19 5.3 Privacy 20 5.4 Automation 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		4.2.1.	Introduction	•	•	•	<u>14</u>
4.2.2.1. Overall TTP 15 4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5.0perational Limitations 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21		<u>4.2.2</u> .	Cobalt Strike	•	•	•	<u>14</u>
4.2.2.2. IoCs 15 4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1. Time and Effort 17 5.1.1. Fragility 17 5.1.2. Discoverability 17 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21		4.2.2.	<u>1</u> . Overall TTP	•	•	•	<u>15</u>
4.2.3. APT33 15 4.2.3.1. Overall TTP 16 4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1. Time and Effort 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21		4.2.2.	<u>2</u> . IoCs		•	•	<u>15</u>
4.2.3.1 Overall TTP 16 4.2.3.2 IoCs 16 5. Operational Limitations 17 5.1. Time and Effort 17 5.1.1 Fragility 17 5.1.2 Discoverability 17 5.2.1 Specificity 19 5.2.2 Dual and Compromised Use 19 5.3.3 Privacy 20 5.4 Automation 21 6.1 Comprehensive Coverage and Defence-in-Depth 21		<u>4.2.3</u> .	APT33				<u>15</u>
4.2.3.2. IoCs 16 5. Operational Limitations 17 5.1. Time and Effort 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		4.2.3.	<u>1</u> . Overall TTP				<u>16</u>
5. Operational Limitations 17 5.1. Time and Effort 17 5.1.1. Fragility 17 5.1.2. Discoverability 17 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		4.2.3.	<u>2</u> . IoCs				<u>16</u>
5.1. Time and Effort 17 5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21 6.1. Comprehensive Coverage and Defence-in-Depth 21	<u>5</u> .	Operatio	onal Limitations				<u>17</u>
5.1.1. Fragility 17 5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6.1. Comprehensive Coverage and Defence-in-Depth 21	5	.1. Time	and Effort				17
5.1.2. Discoverability 18 5.2. Precision 19 5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		5.1.1	. Fragility				17
5.2. Precision 19 5.2.1 Specificity 19 5.2.2 Dual and Compromised Use 19 5.3 Privacy 20 5.4 Automation 21 6. Best Practice 21 6.1 Comprehensive Coverage and Defence-in-Depth 21		5.1.2	Discoverability		÷		18
5.2.1. Specificity 19 5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		5.2. P	recision		÷		19
5.2.2. Dual and Compromised Use 19 5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		5.2.1	. Specificity				19
5.3. Privacy 20 5.4. Automation 21 6. Best Practice 21 6.1. Comprehensive Coverage and Defence-in-Depth 21		5.2.2	. Dual and Compromised Use		÷		19
5.4 Automation 21 6 Best Practice 21 6.1 Comprehensive Coverage and Defence-in-Depth 21		5.3. P	rivacv				20
6. Best Practice 21 6.1 Comprehensive Coverage and Defence-in-Depth 21		5.4. A	utomation				21
6.1. Comprehensive Coverage and Defence-in-Depth		6. Best	Practice				21
		<u>6.1</u> . C	comprehensive Coverage and Defence-in-Depth				21
<u>6.2</u> . Security Considerations \ldots \ldots \ldots \ldots \ldots \ldots $\frac{24}{2}$		<u>6.2</u> . S	ecurity Considerations				24
<u>7</u> . Conclusions		 Concl 	usions				24

What are loCs?

- IPv4 and IPv6 addresses in network traffic.
- DNS domain names in network traffic, resolver caches or logs.
- TLS Server Name Indication values in network traffic.
- Code signing certificates in binaries or TLS certificate information (such as SHA256 hashes) in network traffic.
- Cryptographic hashes (e.g. MD5, SHA1 or SHA256) of malicious binaries or scripts when calculated from network traffic or file system artefacts.
- Attack tools (such as Mimikatz) and their code structure and execution characteristics.
- Attack techniques, such as Kerberos golden tickets, which can be observed in network traffic or system artefacts.

Pyramid of pair



IoC Lifecycle

- New section based on feedback
 - Discovery
 - Assessment
 - Sharing
 - Deployment
 - Detection
 - Reaction
 - End of Life

Questions/Next Steps

- Further feedback and comments welcome from this group
- Is the work in scope for opsec?
- Would the group consider WG adoption?