掘金行动（Operation Gold Hunting） — 目标瞄准前沿科技行业

ti.dbappsecurity.com.cn/blog/index.php/2020/11/12/operation-gold-hunting/

猎影实验室 November 12, 2020

摘要

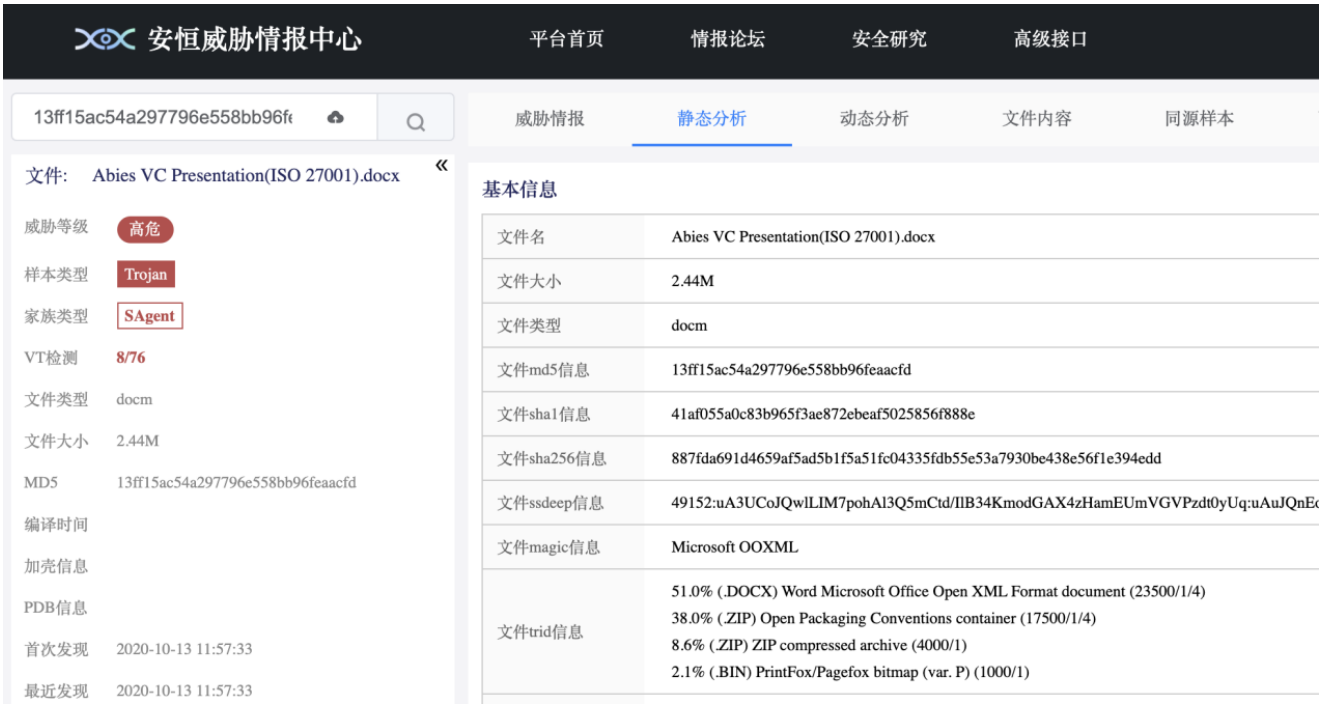
近期，安恒威胁情报中心猎影实验室监测捕获到一些以创投为主题的钓鱼文档。诱饵文档标题伪装成创投资本的保密协议，利用模板注入下载后续内容，同时伪造创投相关文档内容诱导迷惑受害者。通过分析发现行动的主要目标集中在风投前沿科技相关行业。

分析

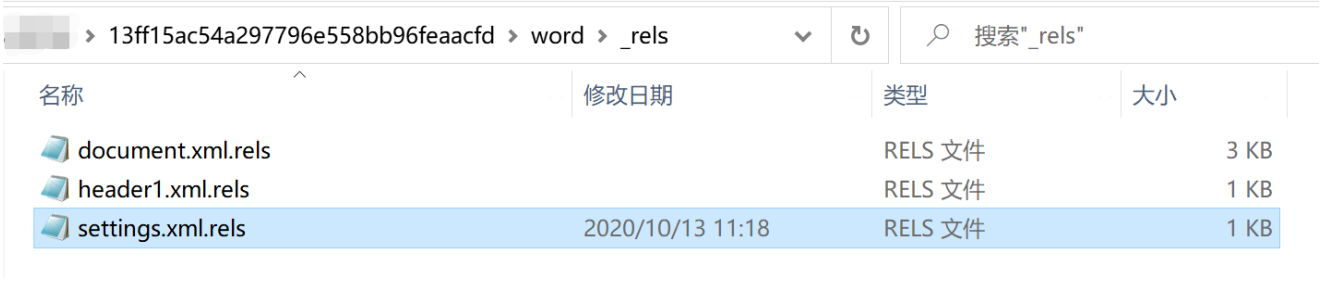
我们捕获到“Union Square Ventures Partnership – Mutual NDA Form.docx”，“Abies VC Presentation(ISO 27001).docx”等多个标题为创投资本相关的文档，其中NDA为Non-Disclosure Agreement缩写，意为保密协议。

样本名称	MD5
Abies VC Presentation (1).docx	ecf75bec770edcd89a3c16d3c4edde1a
Digital Asset Investment Stategy 2020 (ISO 27001).docx	bcf97660ce2b09cbffb454aa5436c9a0
Abies VC Presentation(ISO 27001).docx	13ff15ac54a297796e558bb96feaacfd
Adviser-Non-Disclosure-Agreement-NDA(ISO 27001).docx	cace67b3ea1ce95298933e38311f6d0b
OKEx and DeepMind Intro Deck(ISO 27001_Protected).docx	645adf057b55ef731e624ab435a41757
Circle Business Introduction(ISO 27001).docx	bde4747408ce3cfdfe8238a133ebcac9
Berkshire Hathaway HomeServices Custody – Mutual NDA.docx	421b1e1ab9951d5b8eeda5b041cb0657
Union Square Ventures Partnership – Mutual NDA Form.docx	d2f08e227cd528ad8b26e9bbe285ae3c
Chiliz Partnership – Mutual NDA Form.docx	04deb35316ebe1789da042c8876c0622
FasterCapital Mutual NDA Form.docx	af4eefa8cddc1e412fe91ad33199bd71
FasterCapital Introduction 2020 Oct.docx	34239a3607d8b5b8ddd6797855f2e827
Lundbergs NDA Mutual Form.docx	389172d2794d789727b9f7d01ec27f75

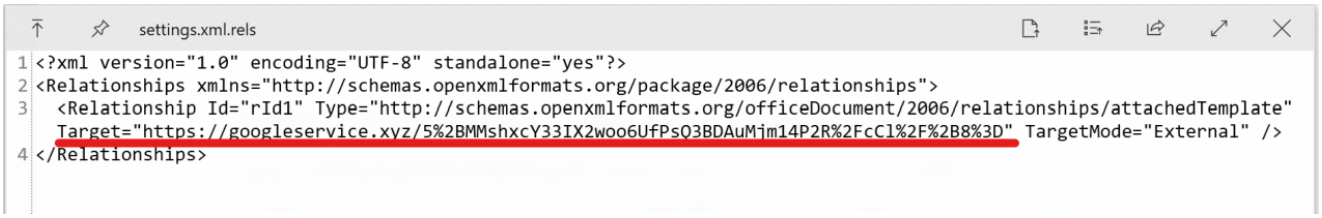
样本形式大致类似，我们这里取其中一个的名为Abies VC Presentation(ISO 27001).docx的样本来分析，意为冷杉创业投资汇报。



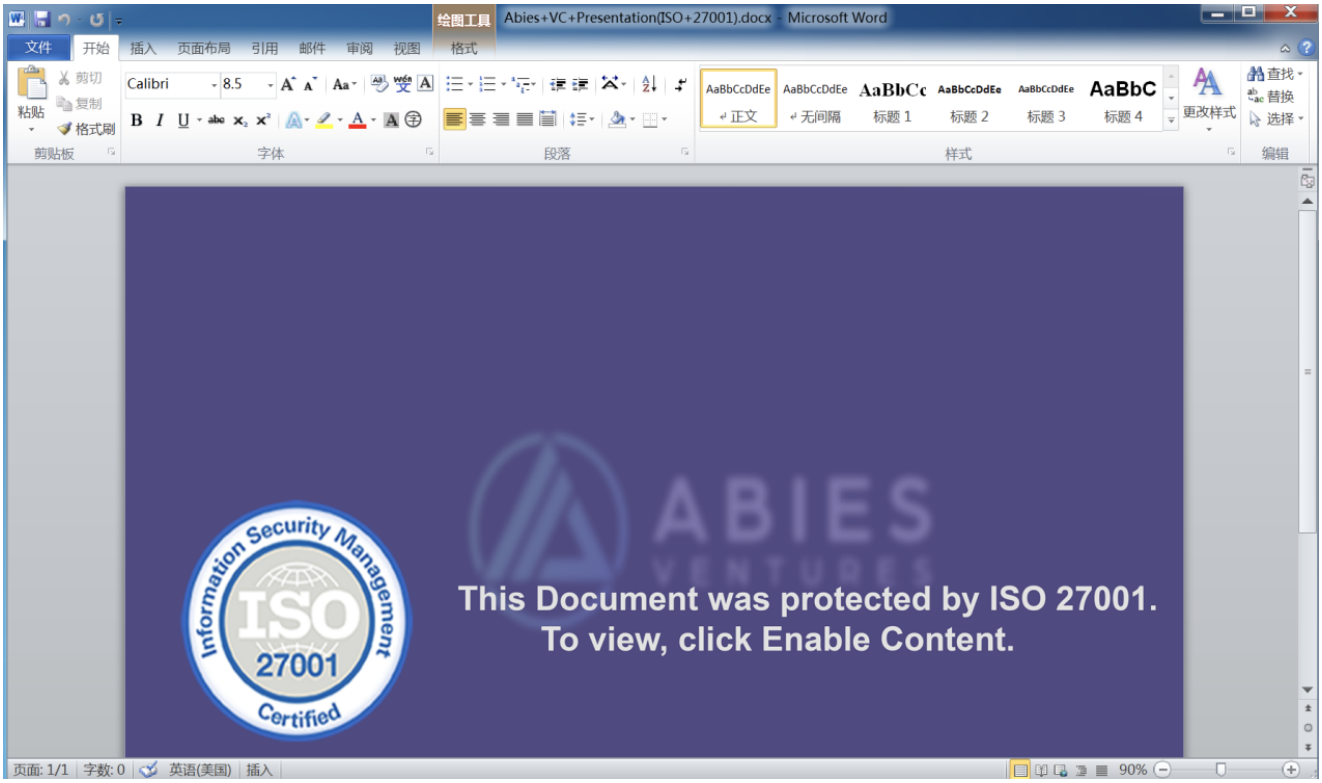
settings.xml.rels文件内包含远程链接，



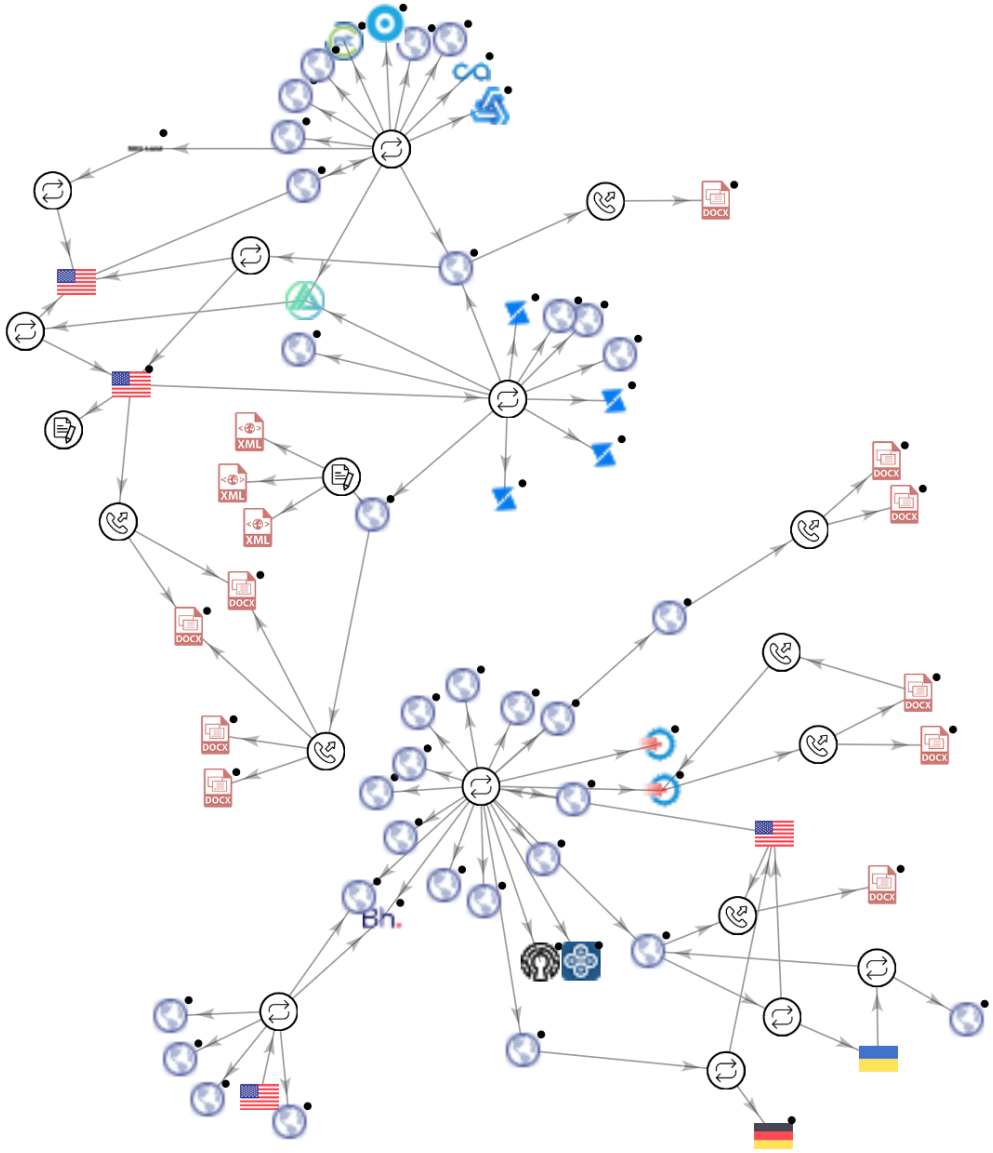
分析的样本在启动阶段会尝试访问https://googleservice[.]xyz/5+MMshxcY33IX2woo6UfPsQ3BDAuMjm14P2R/cCl/+8=下载后续恶意文件，目前此链接无法访问，



文档的内容为伪装的ISO 27001标准保密协议，在ISO 27001标准的logo下有被盖住的冷杉创投的logo，且包含诱导受害者点击的相关信息。



对样本所使用的网络资产进行关联分析，我们找到了不少相关网络资产。



可以看到关联到了这次攻击中所伪装的冷杉投资的相关域名，abiesvc[.]com、abiesvc[.]info

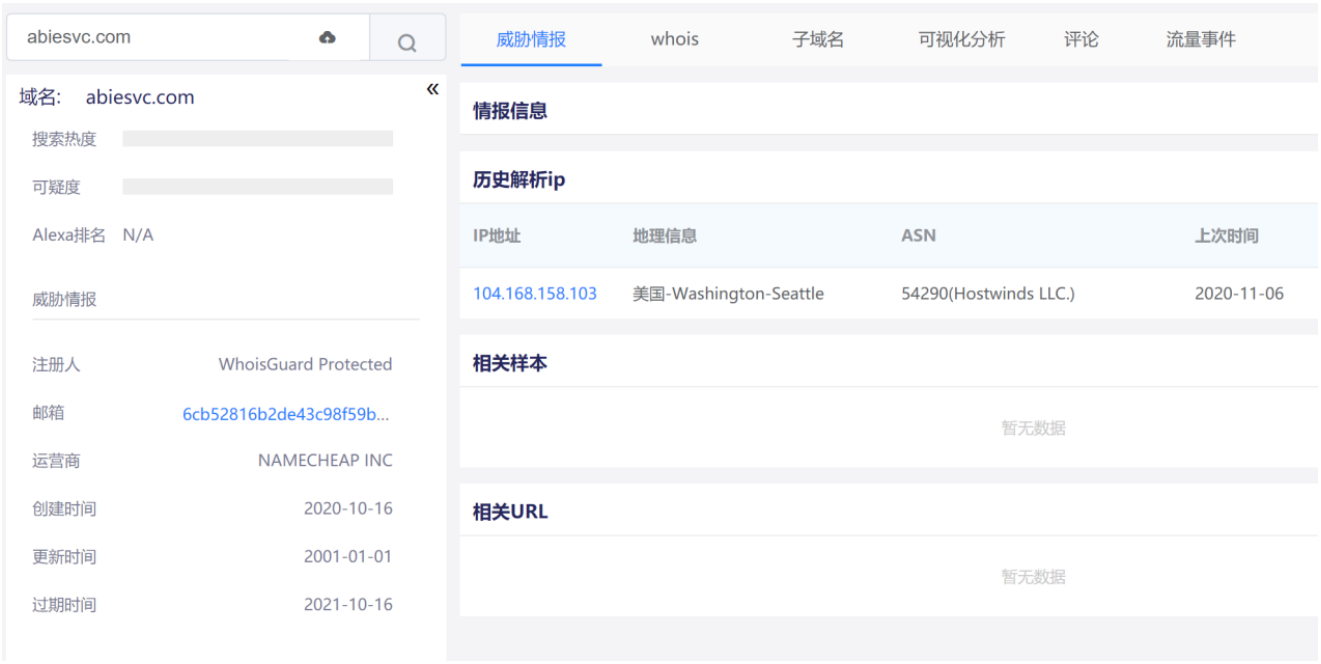
× 104.168.160.6

SUMMARY DETECTION DETAILS RELATIONS COMMUNITY

Passive DNS Replication

Date resolved	Domain
2020-10-16	isosecurity.xyz
2020-10-16	abiesvc.com
2020-09-30	abiesvc.info
2020-09-03	deepmind.fund
2020-08-05	googleservice.xyz
2020-08-03	googleservice.icu
2020-08-02	circlecapital.us

域名的注册时间都不久。

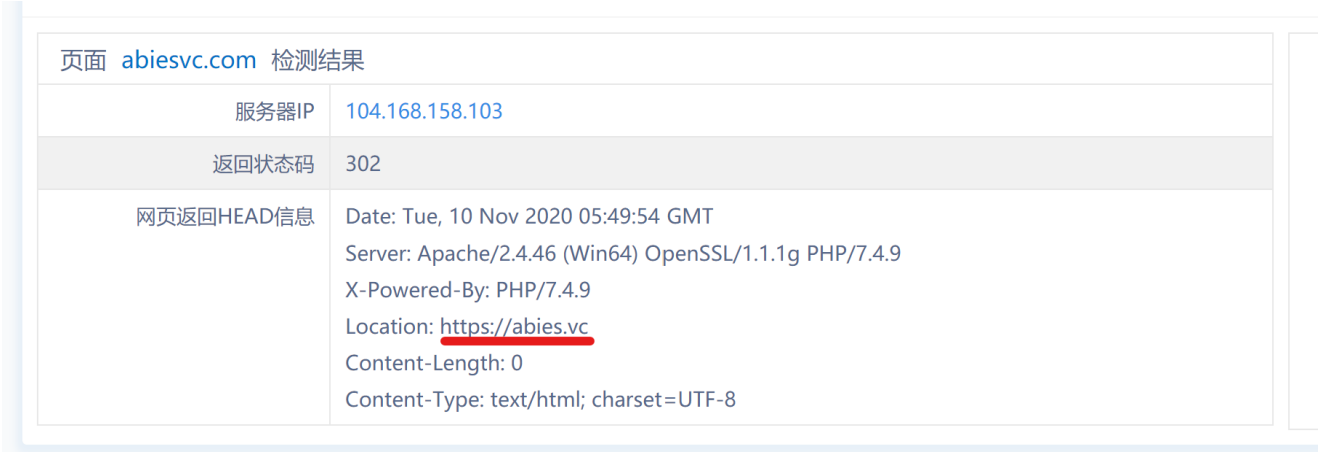


类似的域名还有lemniscap[.]cc、dekryptcap[.]digital、fastercapital[.]cc、lundbergs[.]cc等创投资本相关域名。注册的域名中有本次样本使用的googleservice[.]xyz以及docstream[.]online、isosecurity[.]xyz、filestream[.]download这类有着欺骗性的域名。也发现了加密货币相关的域名coinbigex[.]com、coinbig[.]dev、galaxydigital[.]cloud、kraken-dev[.]com等和能源投资相关域名innoenergy[.]info

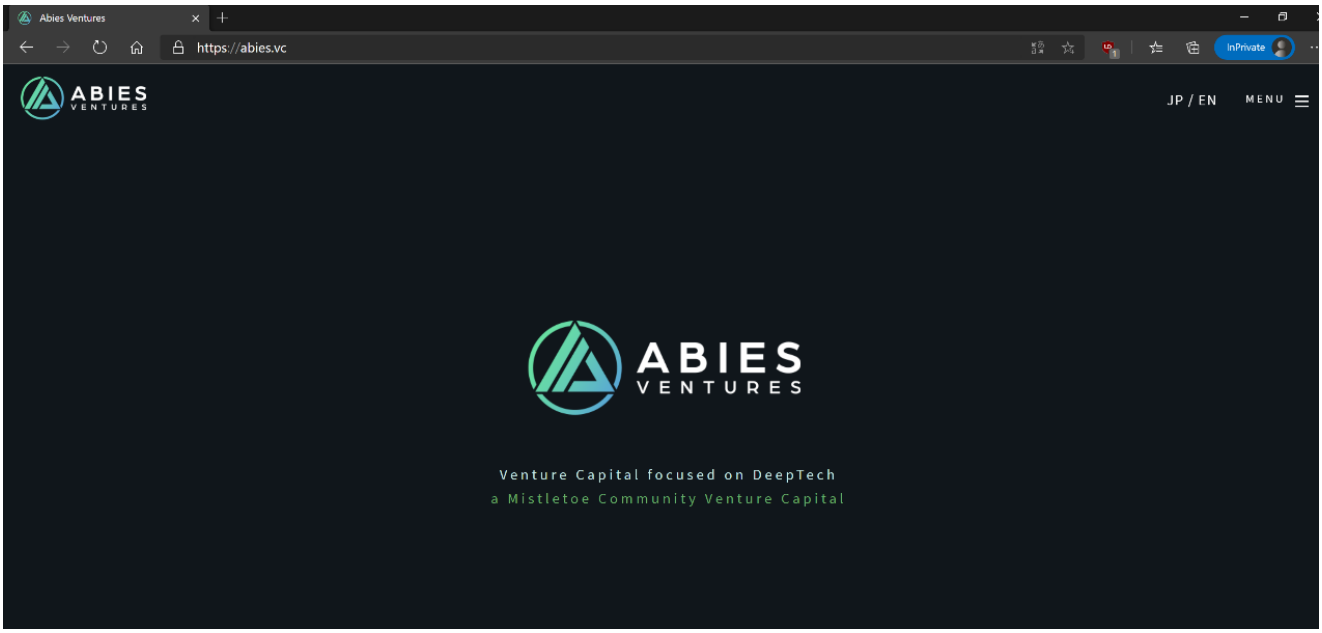
持有域名	伪装公司	主要经营/投资领域

abiesvc[.]com	AbiesVentures	前沿科技
abiesvc[.]info		
lemniscap[.]cc	LemnisCapital	加密资产、区块链
dekryptcap[.]digital	DekryptCapital	区块链、隐私保护技术
coinbigex[.]com	Coinbig Limited	区块链
coinbig[.]dev		
fastercapital[.]cc	FasterCapital	IT初创公司孵化
innoenergy[.]info	InnoEnergy	清洁能源
galaxydigital[.]cloud	Galaxy Digital	加密货币、区块链
circlecapital[.]us	Circle Capital	互联网、金融
deepmind[.]fund	Deepmind	深度学习
kraken-dev[.]com	Kraken	加密货币交易

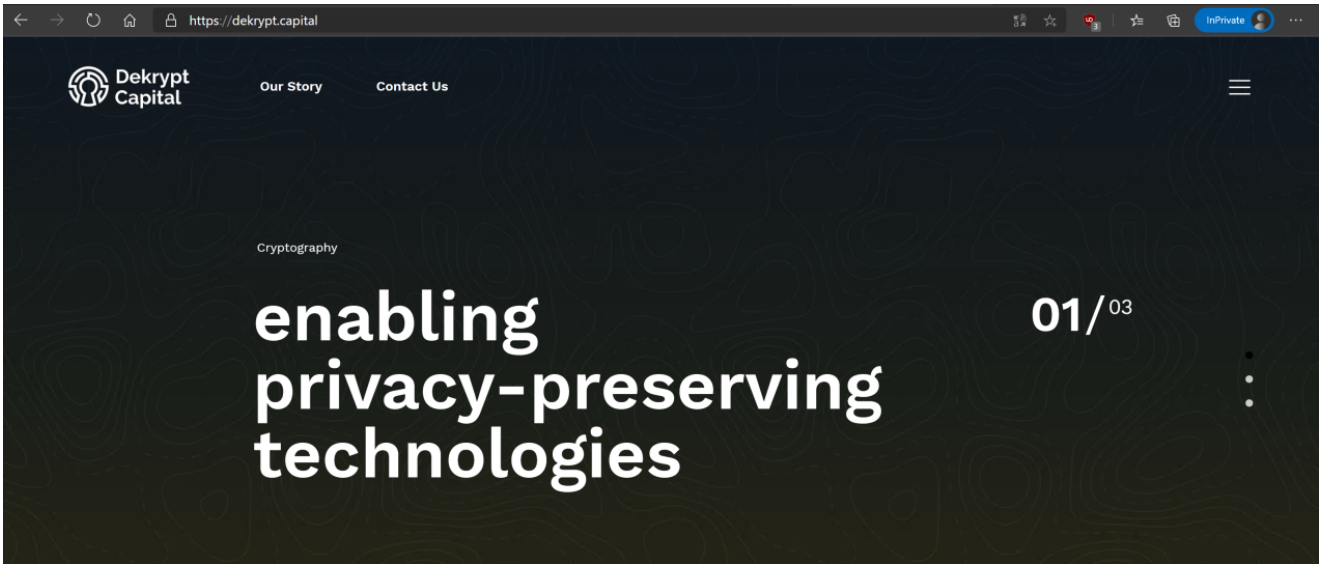
对部分域名做了302的临时重定向，定向至官方网站域名，以增强迷惑性



例如，访问abiesvc[.]com所在域名回重定向至冷杉创投官方网站abies[.]vc



访问dekryptcap[.]digital会重定向至dekryptcapital官方网站dekrypt[.]capital



关联所得到的样本中部分样本的docID相同，docID值位于settings.xml文件内。

样本名称	docID
Abies VC Presentation (1).docx	{861123BC-1DAC-4C24-964C-E9447C597276}
Digital Asset Investment Stategy 2020 (ISO 27001).docx	{861123BC-1DAC-4C24-964C-E9447C597276}
Abies VC Presentation(ISO 27001).docx	{861123BC-1DAC-4C24-964C-E9447C597276}

Adviser-Non-Disclosure-Agreement-NDA(ISO 27001).docx	{861123BC-1DAC-4C24-964C-E9447C597276}
OKEx and DeepMind Intro Deck(ISO 27001_Protected).docx	{1F179ADB-02CF-4A51-820D-20B798FDFF46}
Circle Business Introduction(ISO 27001).docx	N/A
Berkshire Hathaway HomeServices Custody – Mutual NDA.docx	{76DBC1C4-9921-4935-B8A9-9B3167BB1700}
Union Square Ventures Partnership – Mutual NDA Form.docx	{76DBC1C4-9921-4935-B8A9-9B3167BB1700}
Chiliz Partnership – Mutual NDA Form.docx	{76DBC1C4-9921-4935-B8A9-9B3167BB1700}
FasterCapital Mutual NDA Form.docx	{0F5E949A-4017-445B-97B7-3CB064E583DF}
FasterCapital Introduction 2020 Oct.docx	{B44EC542-F37B-44A7-A5B3-617396920BEF}
Lundbergs NDA Mutual Form.docx	{81D6A9AD-4211-4696-97A5-6897FE7766B7}

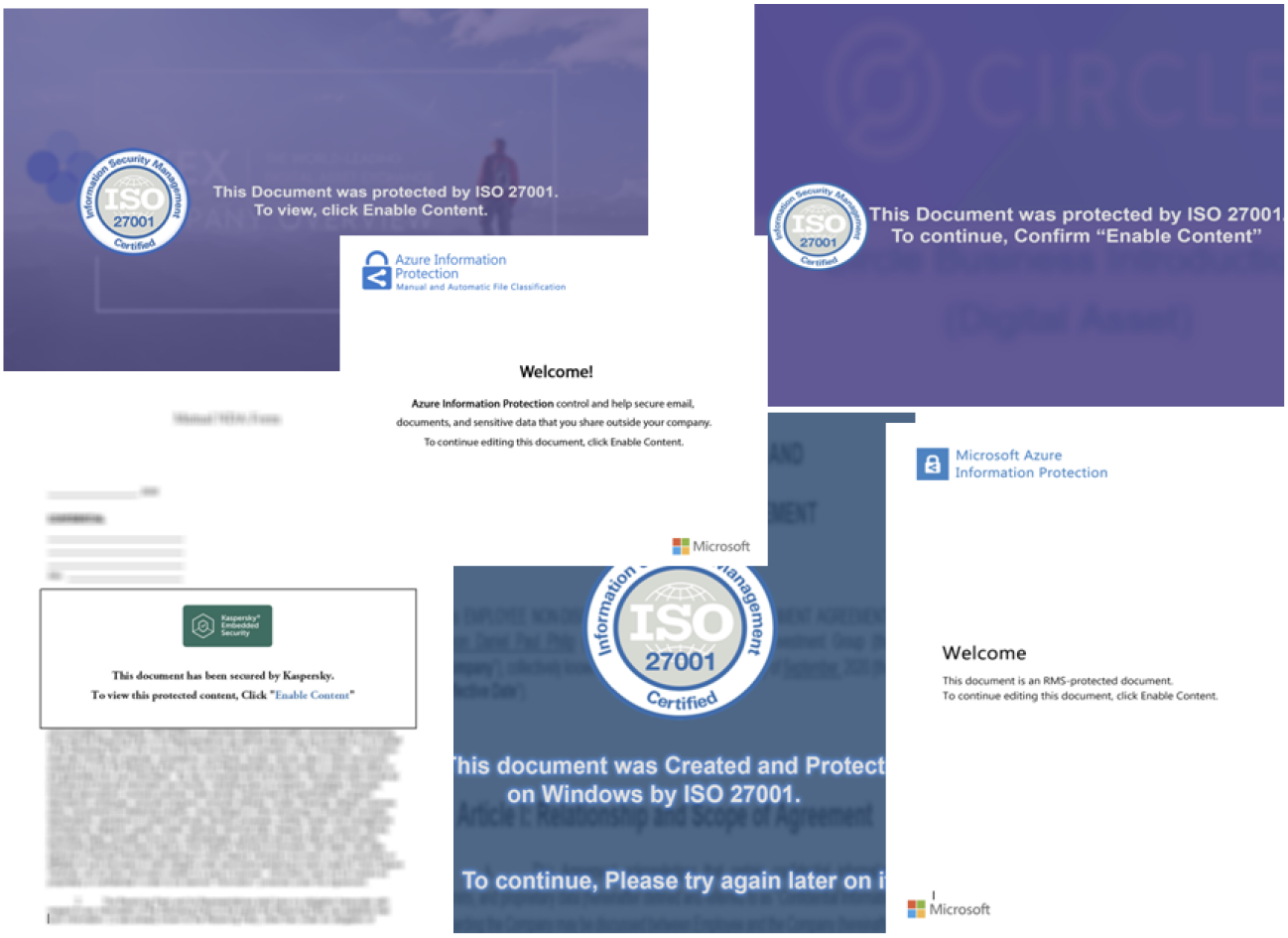
在其中三个关联样本中我们发现了语言值信息。”Lundbergs NDA Mutual Form.docx”的语言值中出现w:eastAsia=”ko-KR”

```
    <m:naryLim m:val="undOvr"/>
  </m:mathPr>
  <w:themeFontLang w:val="en-US" w:eastAsia="ko-KR"/>
  <w:clrSchemeMapping w:followedHyperlink="followedHyperlink" w:hyperlink="hyperlink"
    w:accent3="accent3" w:accent2="accent2" w:accent1="accent1" w:t2="dark2" w:bg2
- <w:shapeDefaults>
    <o:shapedefaults spidmax="1032" v:ext="edit"/>
  - <o:shapelayout v:ext="edit">
      <o:idmap v:ext="edit" data="1"/>
    </o:shapelayout>
  </w:shapeDefaults>
```

“Circle Business Introduction(ISO 27001).docx”样本中发现了语言值w:eastAsia=”ja-JP”；“FasterCapital Introduction 2020 Oct.docx”样本中出现了语言值w:eastAsia=”zh-CN”

```
        <m:naryLim m:val="undOvr" />
    </m:mathPr>
    <w:themeFontLang w:val="en-US" w:eastAsia="ja-JP"/>
    <w:clrSchemeMapping w:followedHyperlink="followedHyperlink" w:hyperlink="hyperlink" w:acc
        w:accent3="accent3" w:accent2="accent2" w:accent1="accent1" w:t2="dark2" w:bg2="lig
  - <w:shapeDefaults>
        <o:shapedefaults spidmax="2049" v:ext="edit"/>
      - <o:shapelayout v:ext="edit">
            <o:idmap v:ext="edit" data="1"/>
        </o:shapelayout>
```

另外除了前面的伪装文档内容外，还有多种伪装文档内容样式。



总结

在分析过程中，我们发现该攻击者注册并掌握了一定数量的创投资本相关域名及一部分其他有欺骗性的域名，同时发现了一批使用创业投资资本保密协议主题的样本，目前捕获的样本显示攻击者的攻击目标集中于前沿科技初创公司。很遗憾目前所有找到的样本的回连地址中尚未发现后续阶段的攻击样本，猎影实验室也将持续关注该攻击事件。

IOC

md5:

ecf75bec770edcd89a3c16d3c4edde1a

bcf97660ce2b09cbffb454aa5436c9a0

13ff15ac54a297796e558bb96feaacfd

cace67b3ea1ce95298933e38311f6d0b

645adf057b55ef731e624ab435a41757

bde4747408ce3cfdfe8238a133ebcac9

421b1e1ab9951d5b8eeda5b041cb0657

d2f08e227cd528ad8b26e9bbe285ae3c

04deb35316ebe1789da042c8876c0622

af4eefa8cddc1e412fe91ad33199bd71

34239a3607d8b5b8ddd6797855f2e827

389172d2794d789727b9f7d01ec27f75

Domains:

googleservice[.]xyz

docstream[.]online

isosecurity[.]xyz

filestream[.]download

coinbigex[.]com

coinbig[.]dev

galaxydigital[.]cloud

kraken-dev[.]com

innoenergy[.]info

lemniscap[.]cc

dekryptcap[.]digital

fastercapital[.]cc

circlecapital[.]us

lundbergs[.]cc

abiesvc[.]com

deepmind[.]fund

abiesvc[.]info

googleservice[.]icu

IP:

104.168.160[.]8

104.168.158[.]224

104.168.160[.]6

104.168.158[.]103